GIGABYTE
TECHNOLOGY

54 Mbps Wireless VPN Router

GN-BR404W

User's Guide

Rev.1.0b Second Edition

Safety, Care and Regulatory Information

Important safety instructions

Read and follow all instructions marked on the product and in the documentation before you operate your system. Retain all safety and operating instructions for future use.

- The product should be operated only from the type of power source indicated on the rating label.
- The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.
- All products hipped with a three-wire electrical grounding-type plug only fits into a grounding-type power outlet. This is a safety feature. The equipment grounding should be in accordance with local and national electrical codes. The equipment operates safely when it is used in accordance with its marked electrical ratings and product usage instructions
- Do not use this product near water or a heat source.
- Set up the product on a stable work surface or so as to ensure stability of the system.
- Openings in the case are provided for ventilation. Do not block or cover these openings. Make sure you provide adequate space around the system for ventilation when you set up your work area. Never insert objects of any kind into the ventilation openings.
- To avoid electrical shock, always unplug all power cables and modem cables from the wall outlets before removing covers.
- Allow the product to cool before removing covers or touching internal components.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with codes for possible special disposal instructions.

Precautions for Products With Modems, Telecommunications, or Local Area Network Options

Observe the following guidelines when working with options:

- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- **CAUTION** - To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Do not plug a modem or telephone cable into the network interface controller (NIC) receptacle.
- Disconnect the modem cable before opening a product enclosure, touching or installing internal components, or touching an uninsulated modem cable or jack.
- Do not use a telephone line to report a gas leak while you are in the vicinity of the leak.
- Do not use this product near water, for example, near a bathtub, washbowl, and

kitchen sink or laundry tub, in a wet basement or near a swimming pool.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neither the provider nor the manufacturer are responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

/ For European users only /

European Community Directive Conformance Statement

This product is in conformity with the protection requirements of EC Council Low Voltage Directive (Safety) 73/23/EEC, EMC Directive 89/336/EEC on the approximation of the laws of the Member States relating to electro-magnetic compatibility.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation. Proposed RF exposure safety information to include in User’s Manual.

Contents

1. INTRODUCTION 1

1-1. CONTENTS OF YOUR SHIPMENT 1
1-2. PHYSICAL INTERFACE 2
1-3. LED INDICATORS 2
1-4. KEY FEATURES 3
1-5. SPECIFICATION 4

2. SYSTEM CONNECTION & INSTALLATION 6

2-1. ADSL/CABLE MODEM REQUIREMENTS 6
2-2. PC HARDWARE REQUIREMENT AT THE PC END 6
2-3. CONNECTION FOR ETHERNET USER 6
2-4. CONNECTION FOR PCMCIA WIRELESS ADAPTER USER 6

3. CONFIGURATION 7

3-1. PREPARATION 7
3-2. SETUP AT YOUR PC END 7
3-2-1. The Settings Under Windows2000 8
3-2-2. Setup Under the Windows 95/98/Me 15
3-2-3. Setup Under Windows XP 21
3-3. SETUP FOR BROADBAND ROUTER 28
3-4. ADVANCED SETUP 48
3-4-1. Network Configuration 48
3-4-2. Wireless Configuration 58
3-4-3. Routing Table 65
3-4-4. Virtual Server 67
3-4-5. Firewall Rule 70
3-4-6. DNS Configuration 74
3-4-7 URL Blocking Configuration 75
3-4-8 VPN Configuration 76
3-5. MANAGEMENT TOOL 79
3-5-1. PPP Monitor 79
3-5-2. Reboot 80
3-5-3. Initilization 81
3-5-4. Change Password 82
3-5-5. Change WAN MAC 83
3-5-6. Upgrade Firmware 84

3-5-7. BackUp Restore *85*
3-5-8. Log Information *86*
3-5-9. Save Maintenance *87*
3-5-10. Ping *88*
3-5-11 Help *89*
3-5-12 About *89*
3-6. STATUS 90
3-7. LOGOUT 95
4. TROUBLESHOOTING 96
APPENDIX A: GLOSSARY 98
APPENDIX B: GENERAL PUBLIC LICENCE 98

1. Introduction

Thank you for using Gigabyte GN-BR404W Wireless-G Broadband Router with VPN. This product comes with high-performance transmission rate and compatible wireless connectivity for either your home or business and will allow you to access the data whenever you want. You will be able to enjoy the freedom that wireless networking delivers.

The IEEE 802.11g standard is designed as a higher-bandwidth - 54M bit/sec - successor to the popular 802.11b, or Wi-Fi standard, which tops out at 11M bit/sec. An 802.11g router will support 802.11b and 802.11g clients.

The GN-BR404W Wireless-G Broadband Router lets you connect IEEE 802.11g or IEEE802.11b devices to the network. With its high-speed data transmissions of up to 54 Mbps, you complete a lot of work in a short amount of time. Network users can share a broadband Internet connection, access e-mail, download large files, videoconference, and distribute and play digital images, videos, and MP3 files. And with up to 152-bit WEP encryption, you can feel relieved that your wireless network communications are private.

It also provides firewall and Virtual Private Networking(VPN) features to protect your local area network when connecting to the Internet. Additionally, GN-BR404W enables you to easily setup all procedures in no time before using this product.

1-1. Contents of Your Shipment

Before the installation procedures, please ensure the components are not damaged during the shipping. The shipment of the GN-BR404W includes:

- One GN-BR404W Wireless-G Broadband Router
- One AC Power Adapter (5V/2A)
- One User Guide
- Two RJ45 cable (one normal；one crossover)
- An embedded GN-WMAG 802.11b/g wireless LAN card
- One Cradle and Wall Mounting kit

Please contact your local distributor or authorized reseller immediately for any missing or damaged components. If you require returning the damaged product, you must pack it in the original packing material or the warranty will be voided.

1-2. Physical Interface

- **Four Ethernet LAN Port**

  RJ-45, Auto-sensing and Auto-MDI/MDIX for 10/100M Ethernet LAN connection

- **One Ethernet WAN Port**

  RJ-45, Auto-sensing for 10/100M Ethernet WAN connection

- **Init Bottom**

  Initial reset (Init to factory default)

- **Power**

  The power port is where you connect the power adapter.

- **External PCMCIA Card Slot**

  Support the Gigabyte GN-WMAG and the GN-WLMA101 Wireless PCMCIA Card.

1-3. LED Indicators

- **Status**

Green light	Power on
Red light	The device is damaged.

- **WAN** (Green light)

On	ADSL/Cable Modem is connected to WAN port.
Blinking	Transmit or receive data via the WAN port.

- **LAN1-LAN4** (Green Light)

On	10/100 Mbps Network Connection
Blinking	10/100 Mbps Data Transmission Rate

- **Wireless** (Green Light)

On	The PCMCIA Card is plugged in.
Blinking	Package transmit
Off	The green light off means No PCMCIA Card installed.

1-4. Key Features

- Two option of plug in wireless card
  - Gigabyte GN-WMAG Wireless LAN Card
  - Gigabyte GN-WLMA101 Wireless LAN Card
- Very High WAN-LAN FTP throughput up to 89.5 Mbps
- Support UPnP and Windows Messenger
- Advanced Smart Setup Support
  - Smart Installation – Automatically detects and connects to your ISP
  - Smart Detection – Automatically detects and changes LAN side IP when LAN-WAN IP conflicts
  - Smart Wizard – Easy set up with interactive install tutorial
- Advanced Network Management support
  - Dynamic IP, Static IP, PPPoE, PPPoE Unnumbered
  - PPPoE Multi Session
  - DHCP server with static and dynamic style
- Advanced Wireless Security support
  - Wi-Fi Protected Access (WPA)
  - 802.1x Secure Wireless Access
  - 64/128/152-bit WEP encryption
  - Access Control List (ACL)
- Advanced Firewall and Parental Control support
  - Stateful Packet Inspection (SPI)
  - Denied of Service (DoS) Protection
  - URL Access Filtering
  - Virtual Server, Stealth Mode, Exposed Host (DMZ)
- Advanced Log Management support
  - Firewall/UPnP/WAN Connection Log
- Advanced Web Management support
  - WAN side Remote Management
  - Web based Firmware upgrade
  - Backup and Restore System Setting
- Extended Distributed Wireless Systems (EDWS) support
  - Wireless Distribution System (WDS) support (Point to Multi-Point and Point to Point)
  - Simultaneous operation of AP and WDS functions
- Virtual Private Network (VPN) Support
  - IPSec, L2TP, PPTP NAT traversal (VPN pass-through)

- ✠ IPSec support remote access VPN (client-to-site), site-to-site VPN
- DNS Relay and Dynamic DNS support
- Static & Dynamic Routing (RIPv1, RIPv2) support

1-5. Specification

System	
Standards	IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), IEEE 802.11b/g (Wireless)
Operating Range	Wireless - Open space: 100 – 300m; Indoor: 30 - 100m
RF – 802.11b	
Frequency Band	2412 ~ 24835 MHz (subject to local regulation)
Modulation Technology	DSSS (Direct Sequence Spread Spectrum)
Modulation Techniques	DBPSK, DQPSK, CCK
Data Rates	11, 5.5, 2, 1 Mbps, auto fallback
Output power	18 dBm @ Nominal Temp Range
Receive Sensitivity	-85 dBm @ 11 Mbps date rate at nominal temperature
Antenna	1 internal antenna support diversity
RF – 802.11g (backward compatible to 802.11b)	
Frequency Band	2412 ~ 24835 MHz (subject to local regulation)
Modulation Technology	OFDM and DSSS
Modulation Techniques	64QAM, 16QAM, QPSK, BPSK, DBPSK, DQPSK, CCK
Data Rates	54, 48, 36, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps, auto fallback
Output power	18 dBm @ Nominal Temp Range
Receive Sensitivity	-68 dBm @ 54 Mbps date rate at nominal temperature
Antenna	1 internal antenna support diversity
Regulatory and Environmental Compliance	
EMC certification	FCC part 15 (USA)
	CE (Europe)
Temperature Range	Operating: 0 ~ 40 degree C, Storage: -20 ~ 65 degree C
Humidity	10% ~ 85% Non-condensing
Mechanical	
LED indicator	Power/Status LED Wireless LED LAN Port LED x 4 WAN Port LED x 1
Power Supply	5V DC 2A

Gross Weight	320g ±5g
Dimension	178 mm * 132 mm * 43 mm

2. System Connection & Installation

The following lists the requirements for the hardware installation.

2-1. ADSL/Cable Modem Requirements

It needs to have ADSL/Cable Modem with RJ-45 connectors.

2-2. PC Hardware Requirement at the PC End

It needs a PC with Ethernet card connection or a PCMCIA wireless adapter.

2-3. Connection for Ethernet User

Step 1. Please prepare an Ethernet cable (RJ- 45) first.
Step 2. Connect the Ethernet cable to the WAN port of the GN-BR404W.
Step 3. Connect an end of the network cable to the ADSL/Cable Modem of the Ethernet connection port.
Step 4. Connect any port of the area network LAN1, 2, 3, & 4 of the GN-BR404W to your PC.
Step 5. Connect the adapter to the power connection slot of the GN-BR404W.
Step 6. Insert the adapter to the power socket.
Step 7. The connection procedure is completed.

2-4. Connection for PCMCIA Wireless Adapter User

Please repeat Steps 1~3 of Section 2-3.

If you use wireless connection, please refer to the wireless card manual which provided by your wireless card manufature. After installing and setting the PCMCIA Wireless Adapter, refer to PC configuration section in Chapter 3, follow the instruction step by step to finish the TCP/IP Protocol setting (Setting PC) .

SSID of the PCMCIA Wireless Adapter should be the same as the SSID of GN-BR404W. The default value is “gigabyte” (or “any”, if your Wireless LAN Card can support.), please do notice the form of the SSID value whether is capital or not.

3. Configuration

3-1. Preparation

Generally speaking, using the GN-BR404W for Internet connection needs the ADSL or Cable service. We assume that you have already obtained the ADSL/Cable service from the local telephone company or the ISP Company, and get the related connection data ready.

Such data include：

a. IP address provided by ISP
b. Subnet mask
c. Default gateway IP address
d. Domain Name System (DNS) Server IP address

- The ISP Company provides the above data.

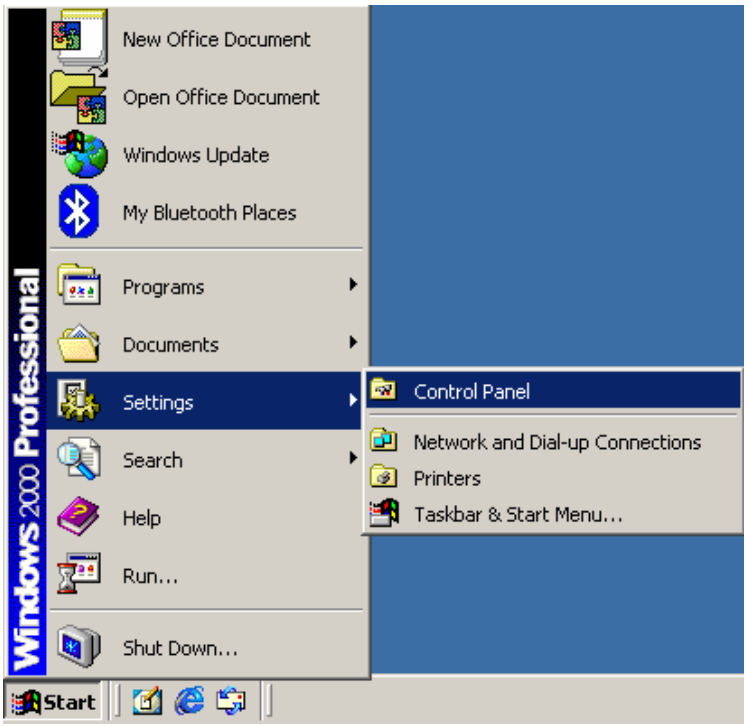
3-2. Setup at Your PC End

An easy-to-use web page setup interface is designed on the GN-BR404W, and the user can perform the setup by the browser. The Gigabyte GN-BR404W Broadband Router presets the IP address as "**192.168.1.254"**, and preset as a DHCP server Please follow the step below to perform the setup under the TCP/IP network environment. Please confirm the TCP/IP communication protocol is installed in your computer (Windows 95/98/Me/NT). If you have not installed the TCP/IP communication protocol, please install it now, and then select your operating system for the setup.

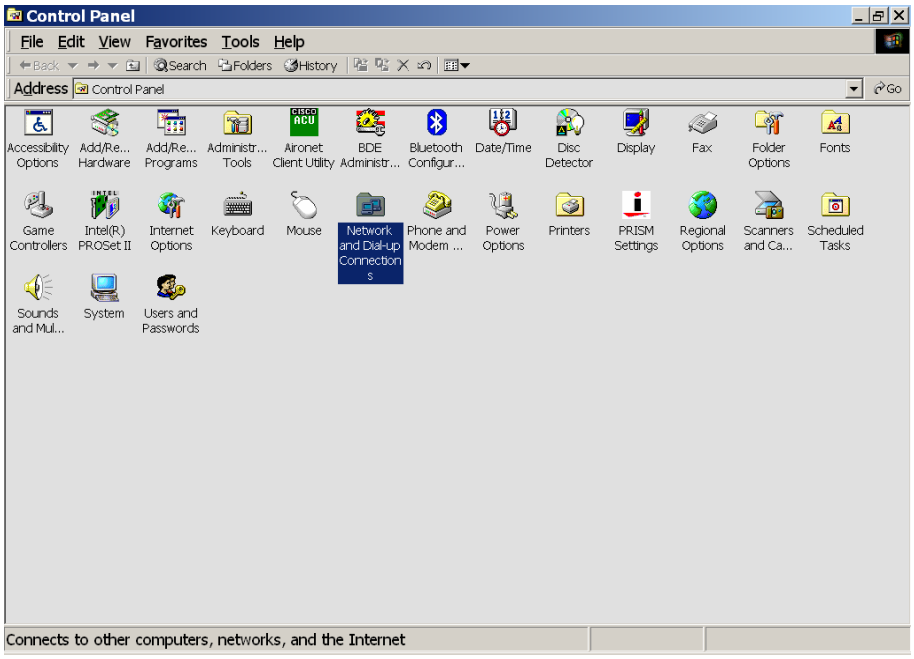
- For Windows 2000, please jump to 3-2-1.
- For Windows 95/98/Me, please jump to 3-2-2.
- For Windows XP, please jump to 3-2-3

3-2-1. The Settings Under Windows2000

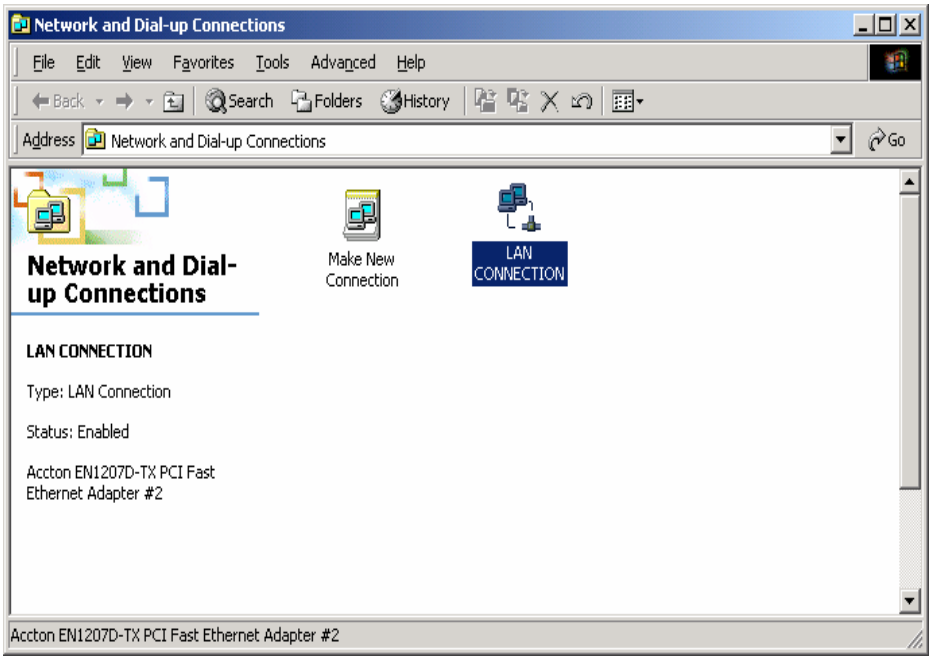
Step 1. Click “**Start**” in the desktop of the Windows to select “**Settings**”, and then click “**Control Panel**”.



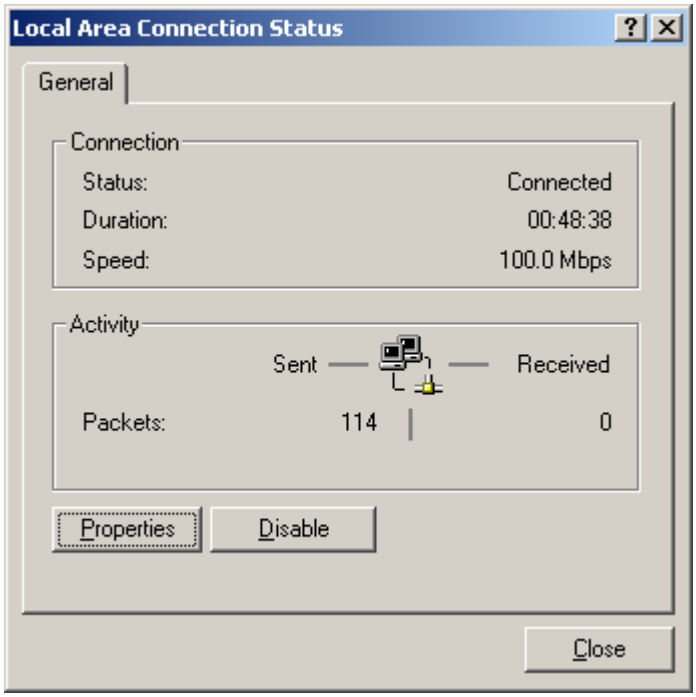
Step 2. Double click the “**Network and Dial-up Connections**”.



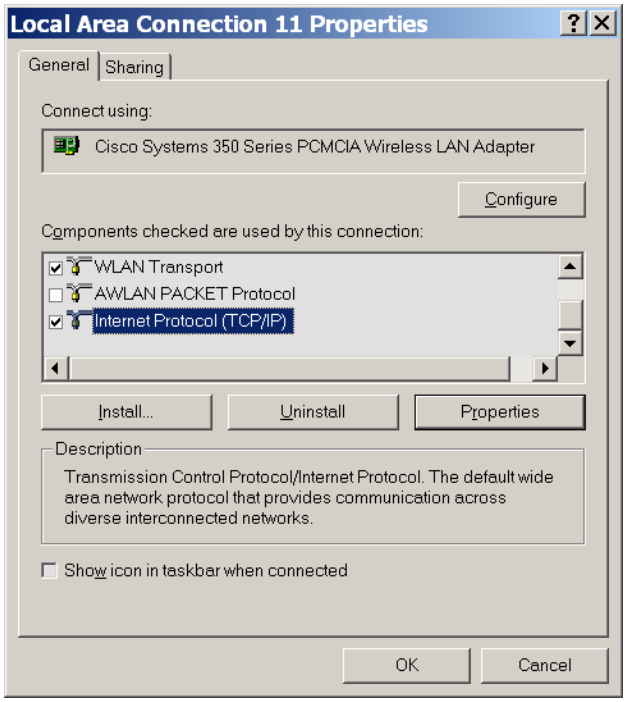
Step 3. Double click the “**LAN CONNECTION**”.



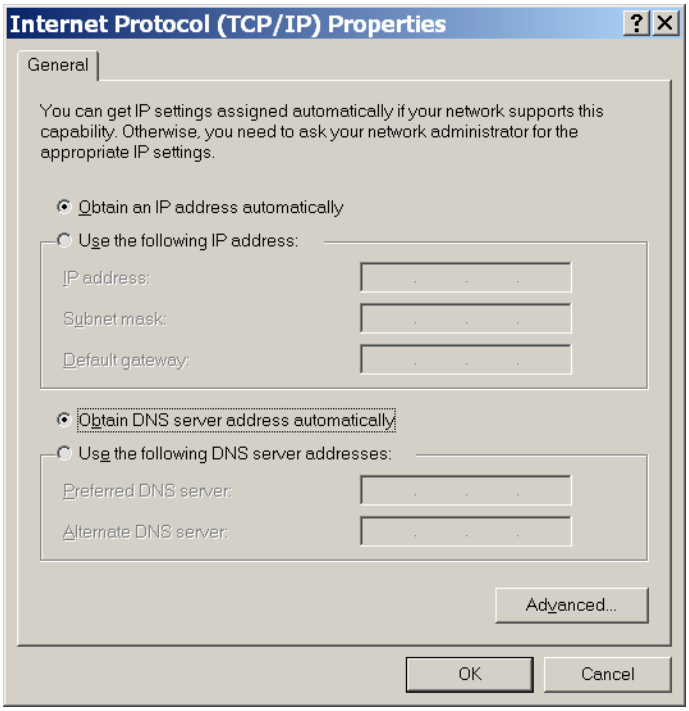
Step 4. Click “**Properties**” in the box under LAN CONNECTION Status.



Step 5. Double click "**Internet Protocol (TCP/IP)**".

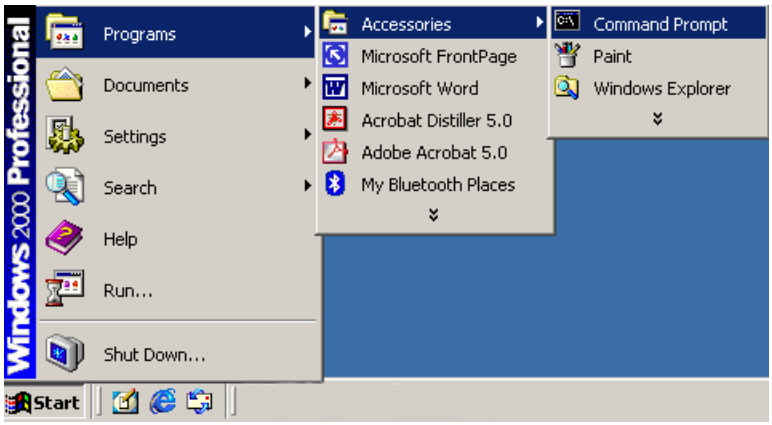


Step 6. Please select "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**", and then press "**OK**".

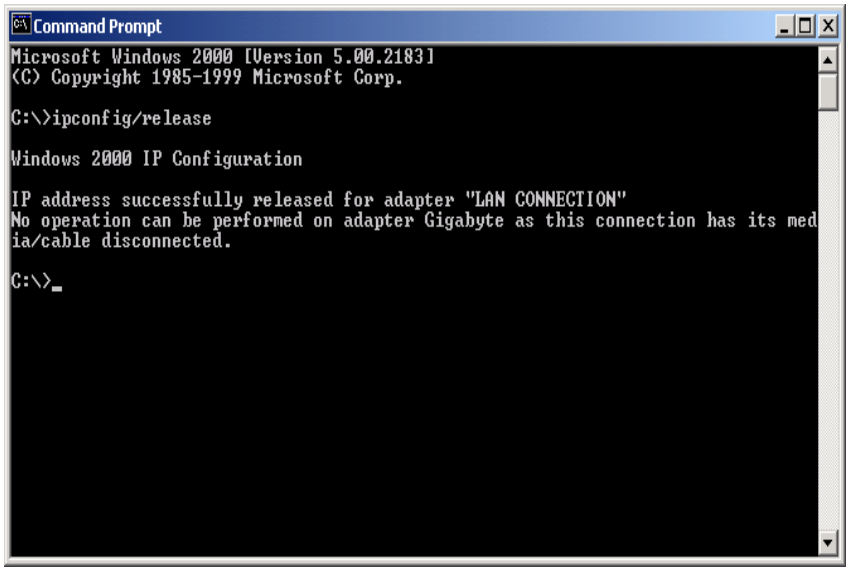


*Now, the computer will obtain an IP address automatically from the GN-BR404W then you can go to "**Step11**" directly. If you would like to obtain an IP address manually, please refer to Step7~Step10.*

Step 7. Click “**Start**” at the desktop of the Windows, and then “**Program**”, “**Accessories**”, and “**Command Prompt**” in sequence.

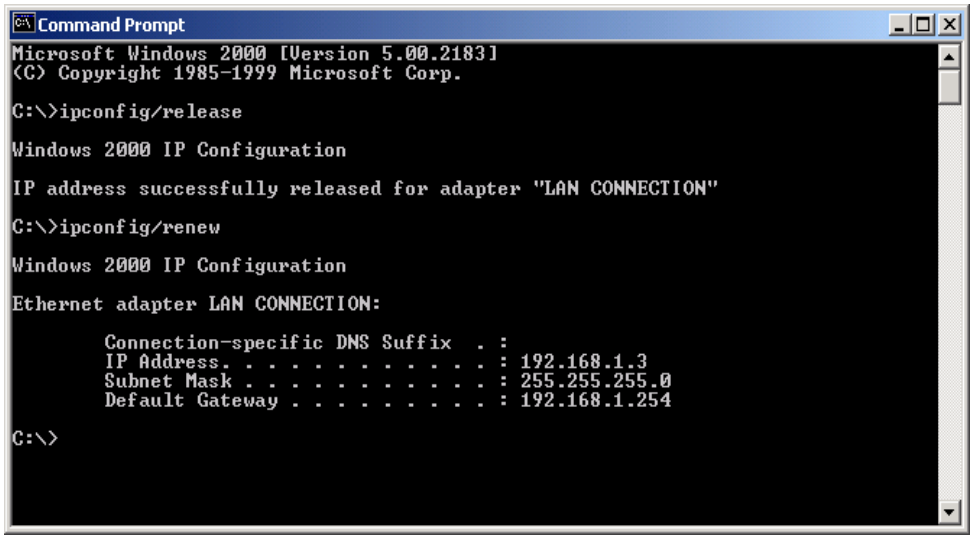


Step 8. Key in the command “**ipconfig/release**” in DOS mode, and then enter.

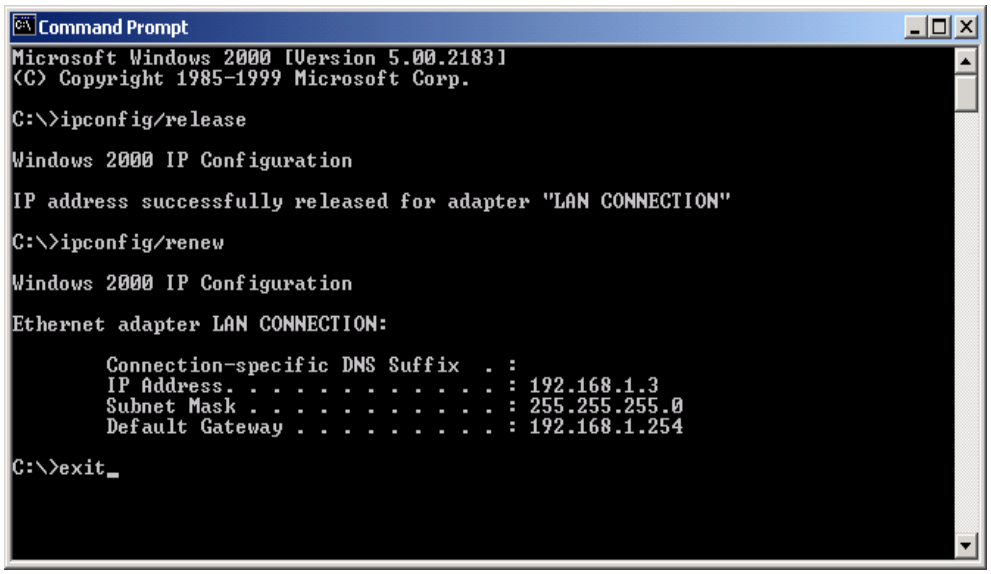


Step 9. Key in the command "**ipconfig/renew**" in DOS mode, and then enter.

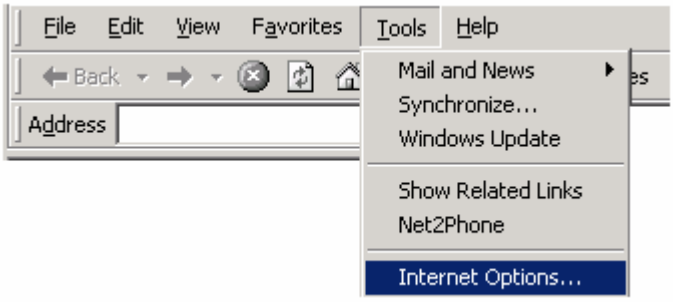
If the IP address of the GN-BR404W is 192.168.1.254, the IP address of your computer must be 192.168.1.X (where "X" is a number between 1 and 253. Each computer on your network must have a different IP address within that range where "X" represents a number between 1 and 253.) The default gateway must be 192.168.1.254.



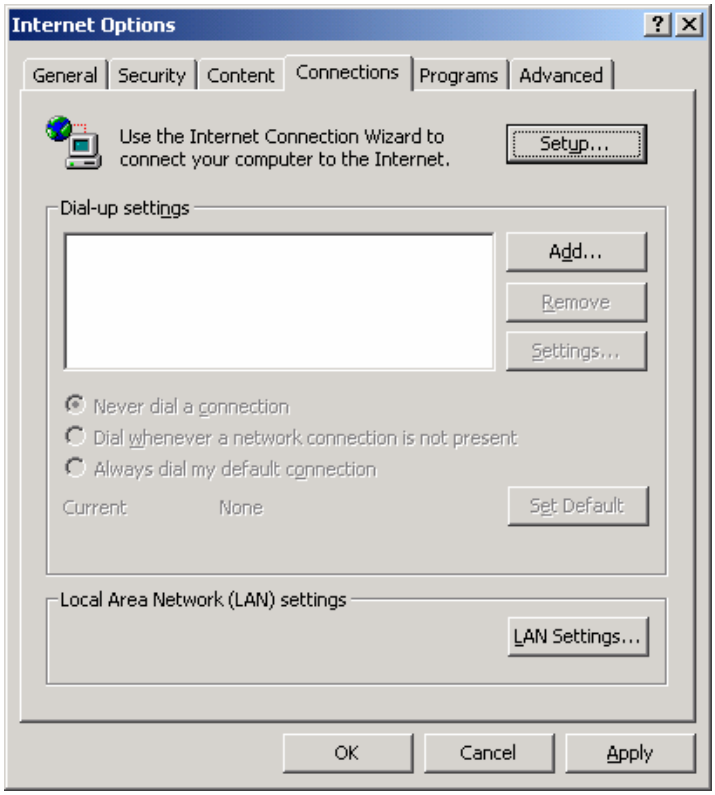
Step 10. Key in the command "**exit**" in DOS mode, and then enter.



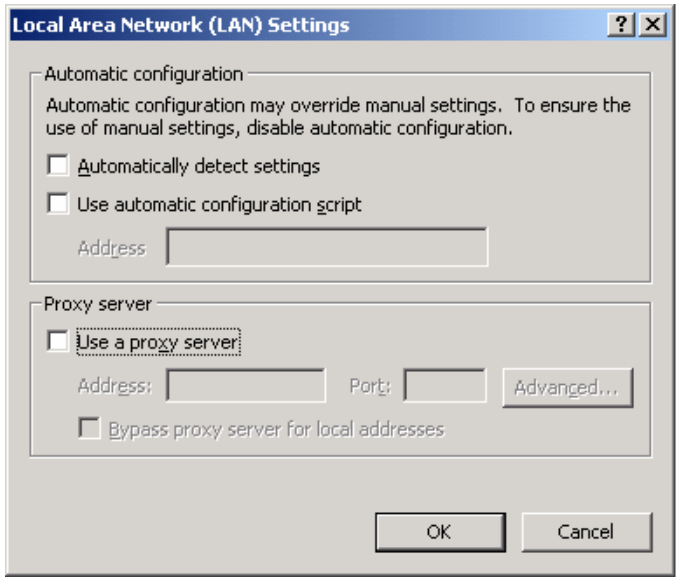
Step11. In your “**Internet Explore**” Browser select “**Internet Options**” under “**Tools**”.



Step 12. In this dialogue box, please click “**Connections**” in the “**LAN Settings**”.



Step 13. Please **DO NOT** tick all of the selection boxes. Press "**OK**" after finishing with the setup, and refer to Section 3-3 for setup of broadband router.

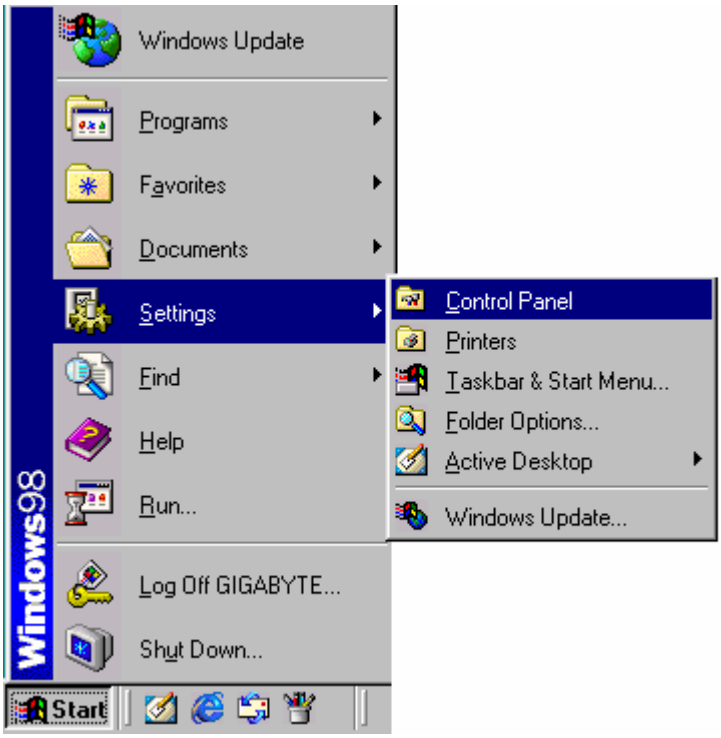


If your ISP Company has a designated Proxy setting, key in the setting after you complete the GN-BR404W configuration.

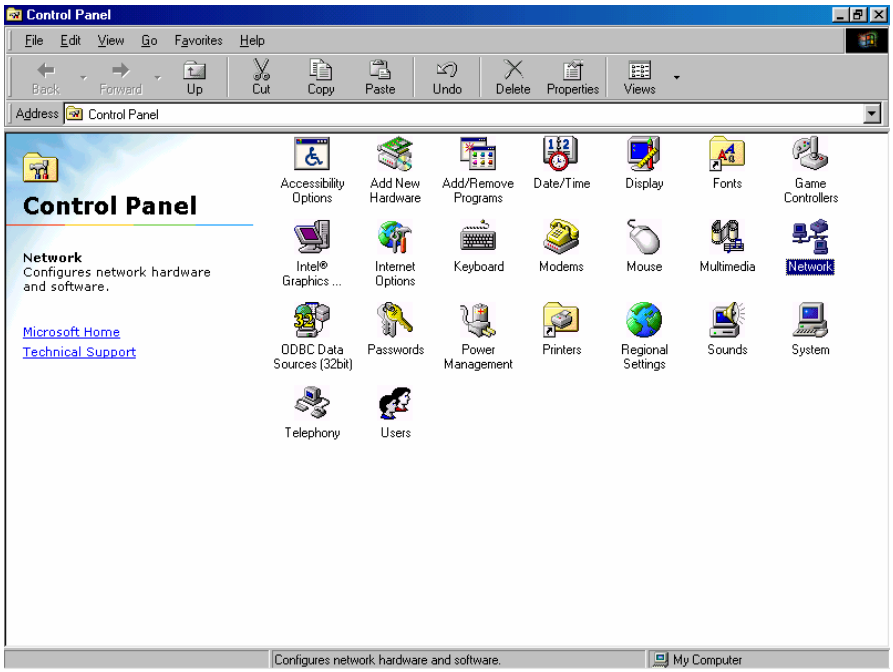
Now, please jump to Section 3-3 to setup broadband router.

3-2-2. Setup Under the Windows 95/98/Me

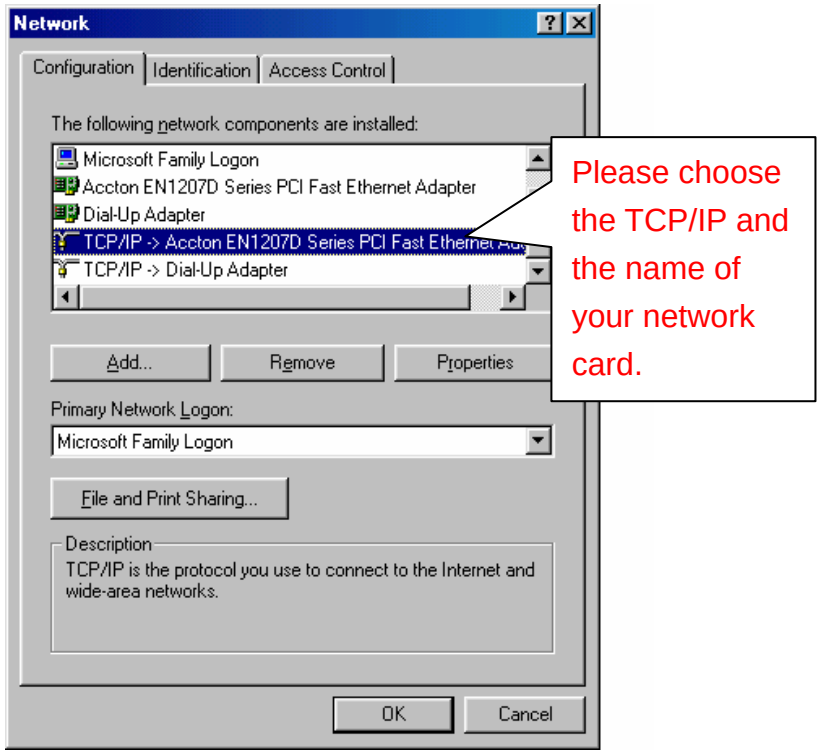
Step 1. Click “**Start**” at the desktop of the Windows, and select “**Settings**”, and then the “**Control Panel**”.



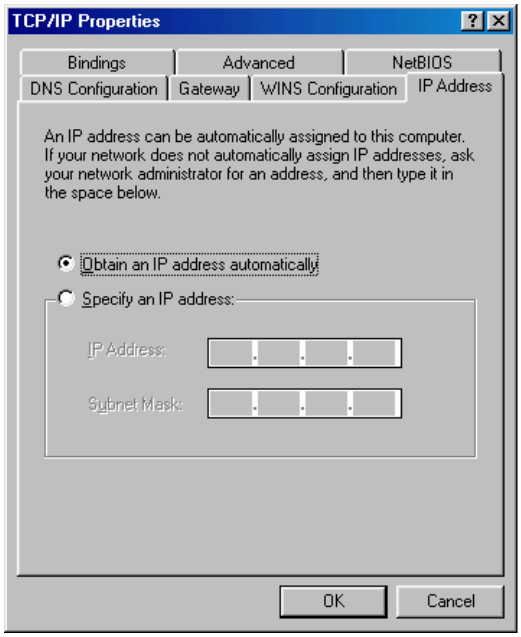
Step 2. Double click “**Network**”.



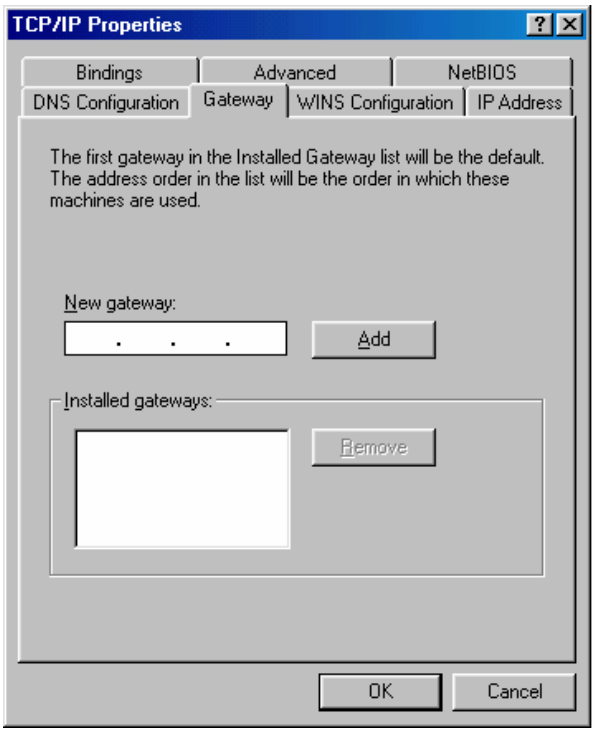
Step 3. Under Network, double click the "**Configuration**", and choose your appropriate setting "**TCP/IP -> and your network card**" below.



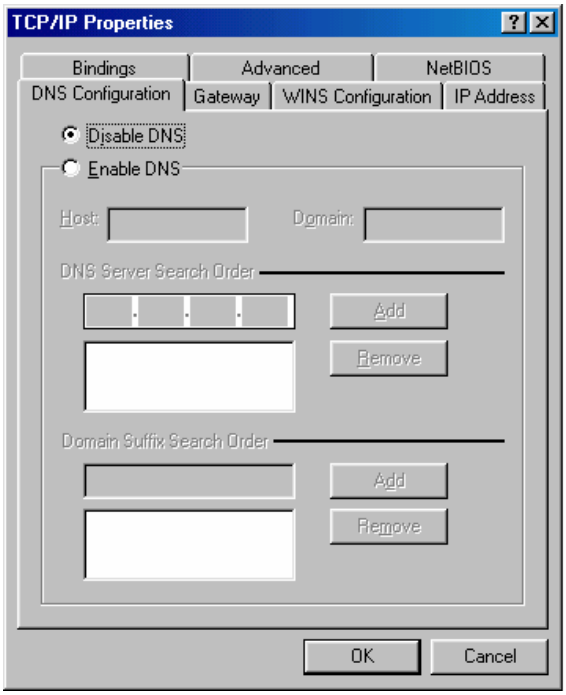
Step 4. Select "**IP Address**" tab. Please select "**Obtain an IP address automatically**" then click "**Gateway**" tab.



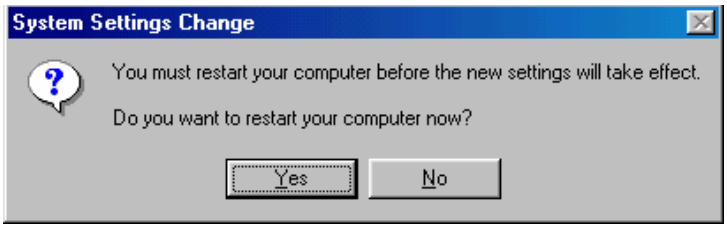
Step 5. In the window of “**Gateway**”, please clear all installed gateways and do not fill any of the blanks, and then click “**DNS Configuration**” tab.



Step 6. In the window of “**DNS Configuration**”, please select “**Disable DNS**” and then press “**OK**”.

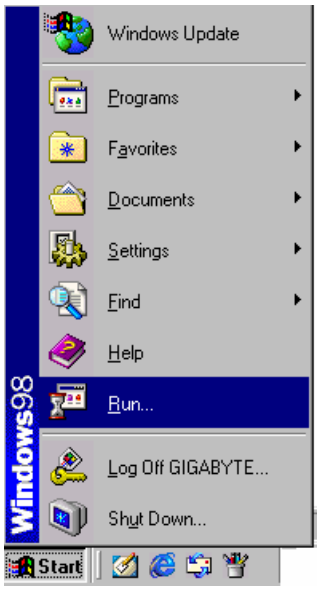


Step 7. Please press “**Yes**”, and reset the computer screen as follows:

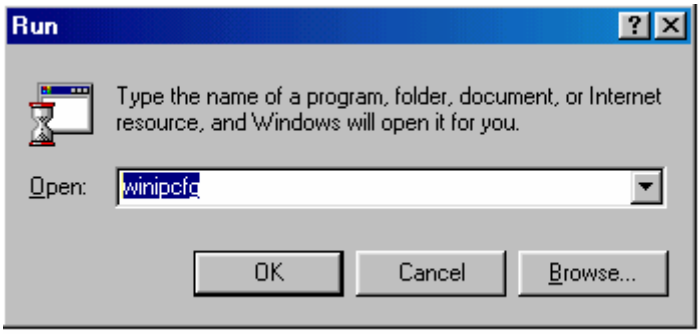


*After booting the computer, the computer will obtain an IP address automatically from the GN-BR404W then you can go to “**Step11**” directly. If you would like to obtain an IP address manually, please refer to Step8~Step10.*

Step 8. After booting the computer, please click “**Start**” and choose “**Run**”.

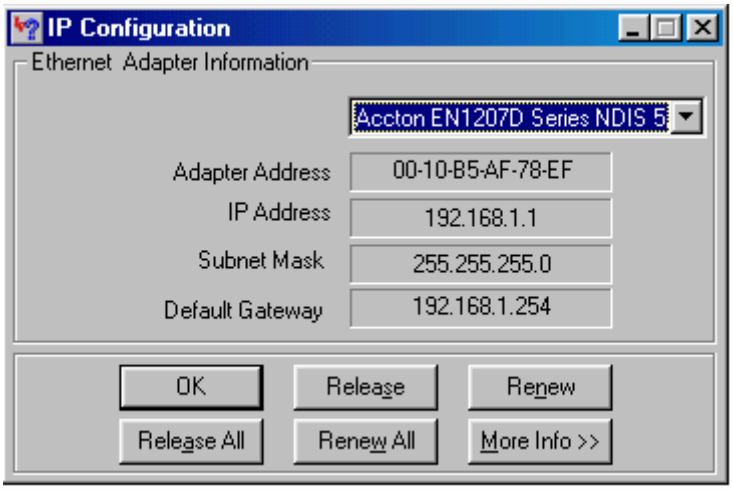


Step 9. Key in “**winipcfg**”, and press “**OK**”.

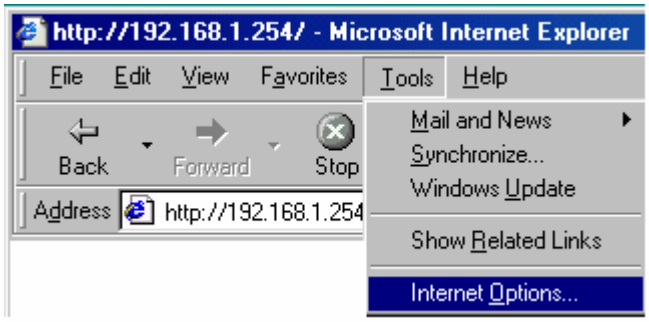


Step 10. In the pulled down menu, select your network card, press “**Release All**”, then press “**Renew All**”, and then press “**OK**”.

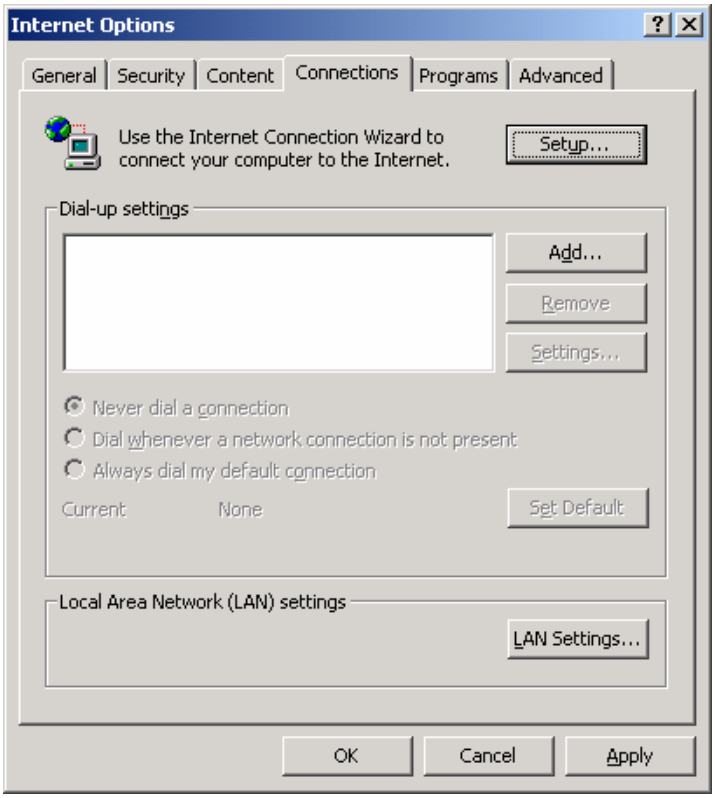
If the IP address of the GN-BR404W is 192.168.1.254, the IP address of your computer must be 192.168.1.X (where “X” is a number between 1 and 253. Each computer on your network must have a different IP address within that range where “X” represents a number between 1 and 253.) The default gateway must be 192.168.1.254.



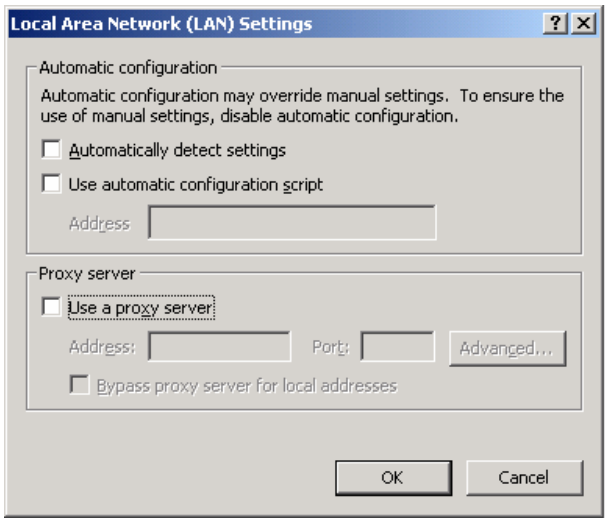
Step11. Please select “**Internet Options**” under “**Tools**” of your IE Browser.



Step 12. In this dialogue box, please select "**Connections**" in the "**LAN Settings**".



Step 13. Please **DO NOT** tick all of the selection boxes. Press "**OK**" after finishing with the setup, and refer to Section 3-3 for setup of broadband router.



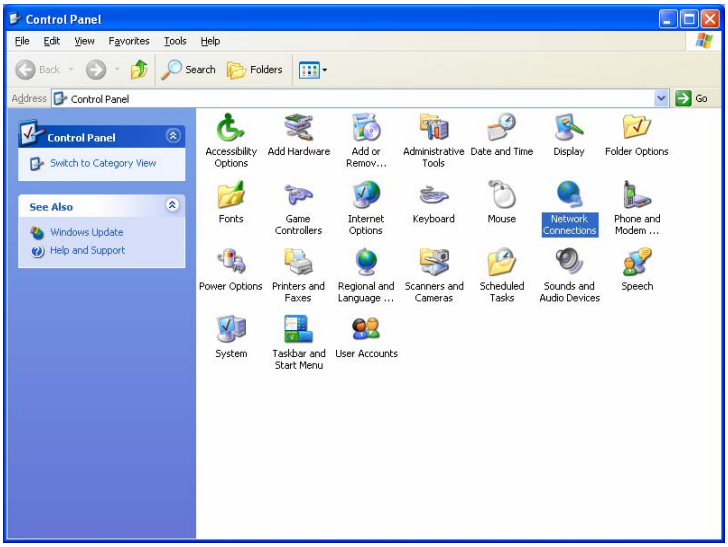
If your ISP Company has a designated Proxy setting, key in the setting after you complete the GN-BR404W configuration.

Now, please jump to Section 3-3 to setup broadband router.

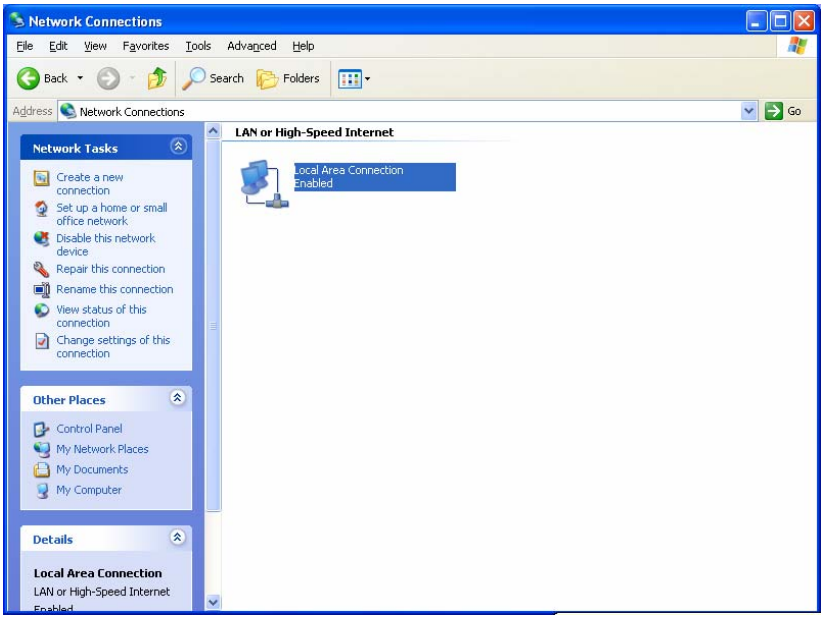
3-2-3. Setup Under Windows XP

Step 1. Click the "**Start**" at the desktop of the Windows, and select the "**Control Panel**".

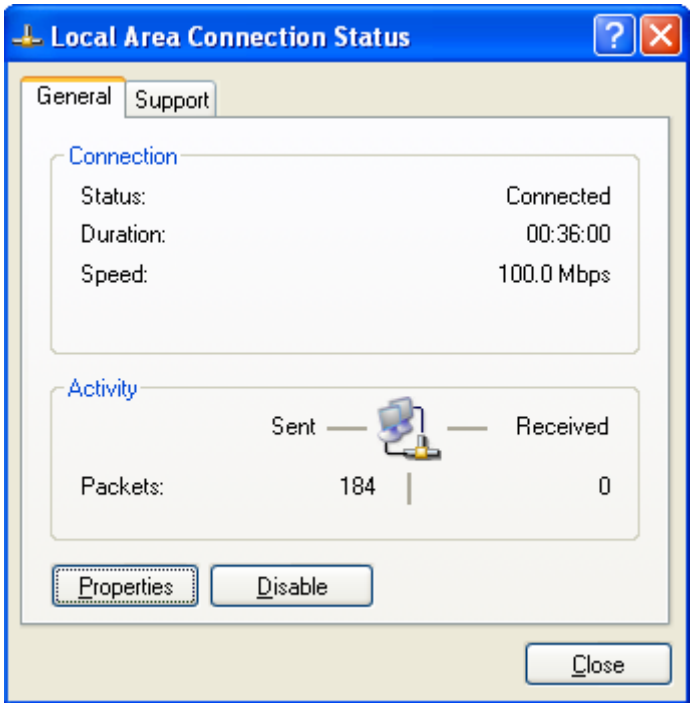
Step 2. Double click the "**Network Connections**".



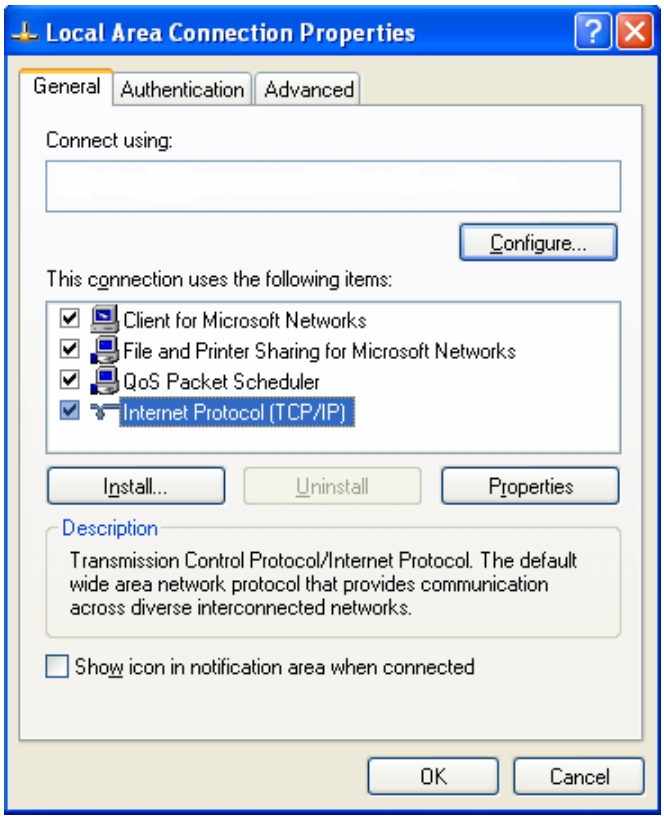
Step 3. Double click the “**Local Area Connection**”.



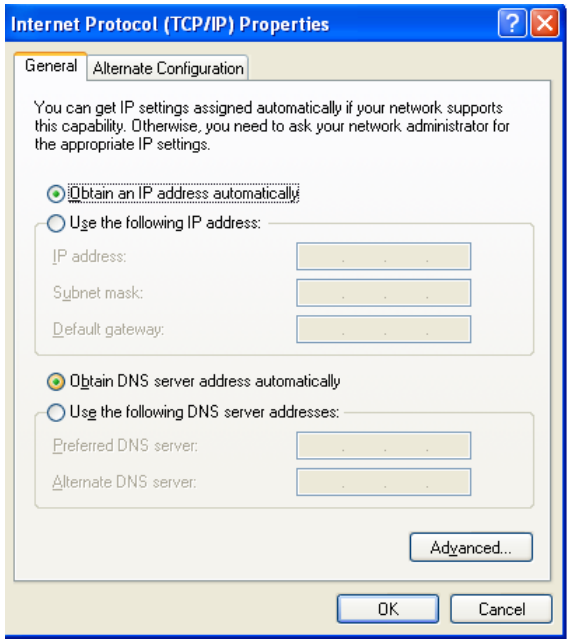
Step 4. Click the “**Properties**” in the box under Local Area Connection Status.



Step 5. Double click the “**Internet Protocol(TCP/IP)**”.

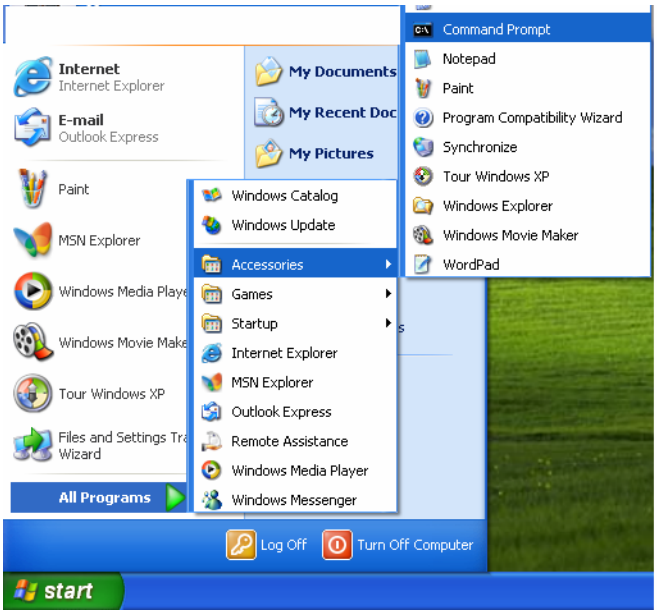


Step 6. Please select the “**Obtain an IP address automatically**” and “**Obtain DNS server address automatically**”, and then press “**OK**”.

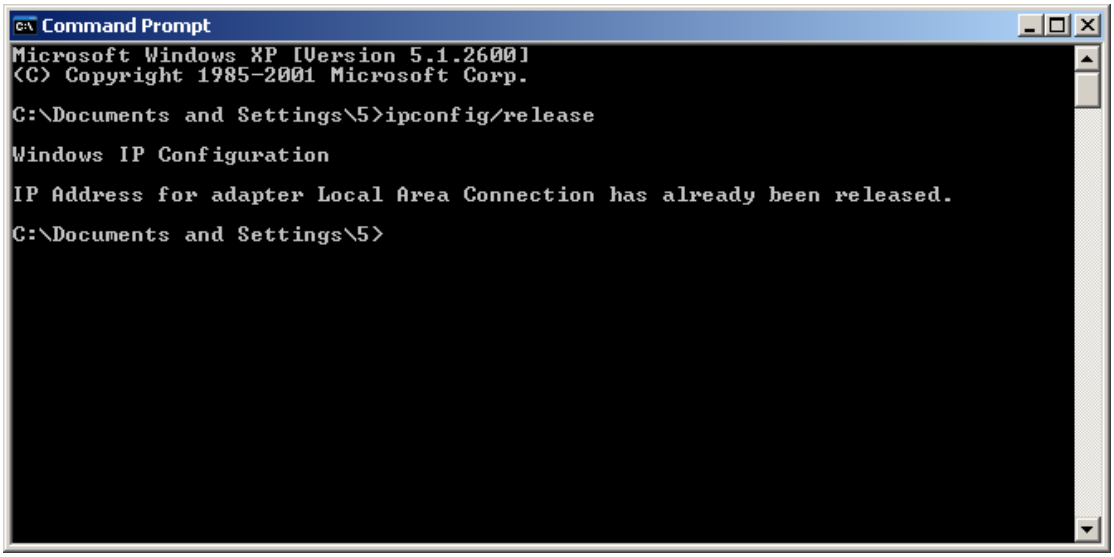


Now, the computer will obtain an IP address automatically from the GN-BR404W then you can go to “Step11” directly. If you would like to obtain an IP address manually, please refer to Step7~Step10.

Step 7. Click the “**Start**” at the desktop of the Windows, and then the “**Accessories**”, and then the “**Command Prompt**”.

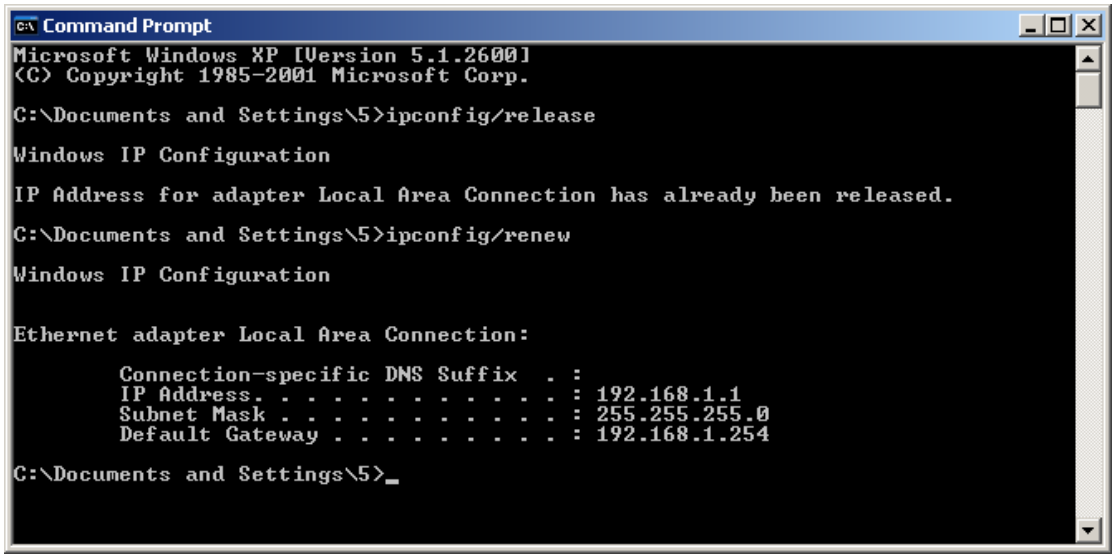


Step 8. Input the “**ipconfig /release**” in the box of Command Prompt, and then enter.

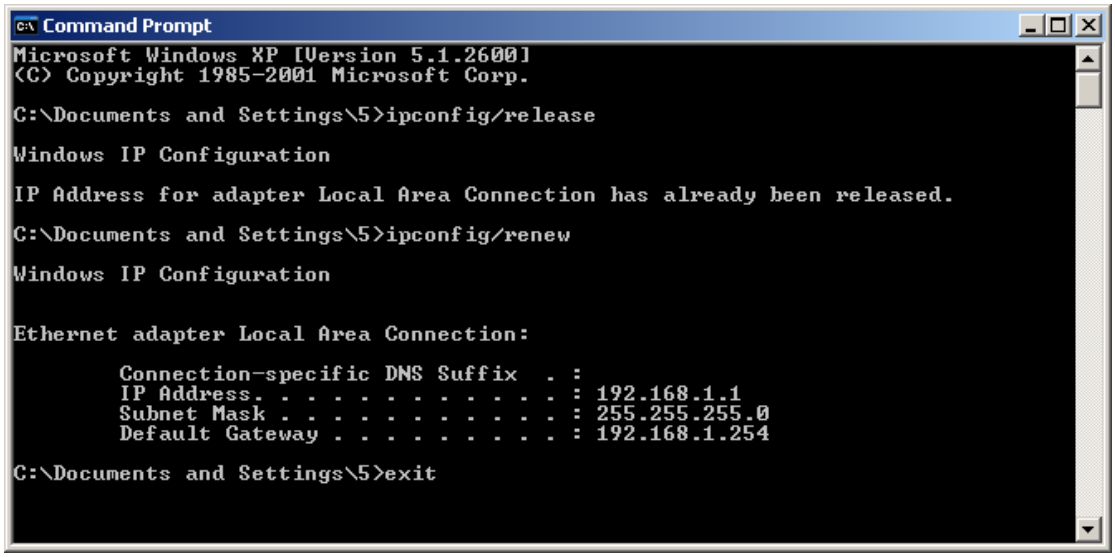


Step 9. Input “**ipconfig/renew**” in the box of Command Prompt, and then enter.

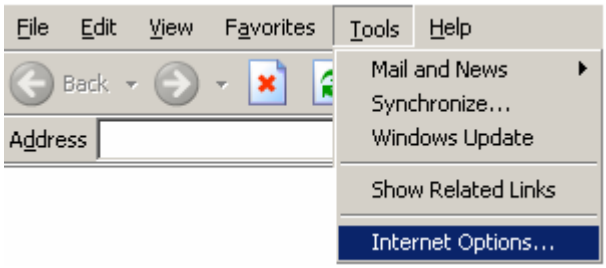
If the IP address of the GN-BR404W is 192.168.1.254, the IP address of your computer must be 192.168.1.X (where “X” is a number between 1 and 253. Each computer on your network must have a different IP address within that range where “X” represents a number between 1 and 253.) The default gateway must be 192.168.1.254.



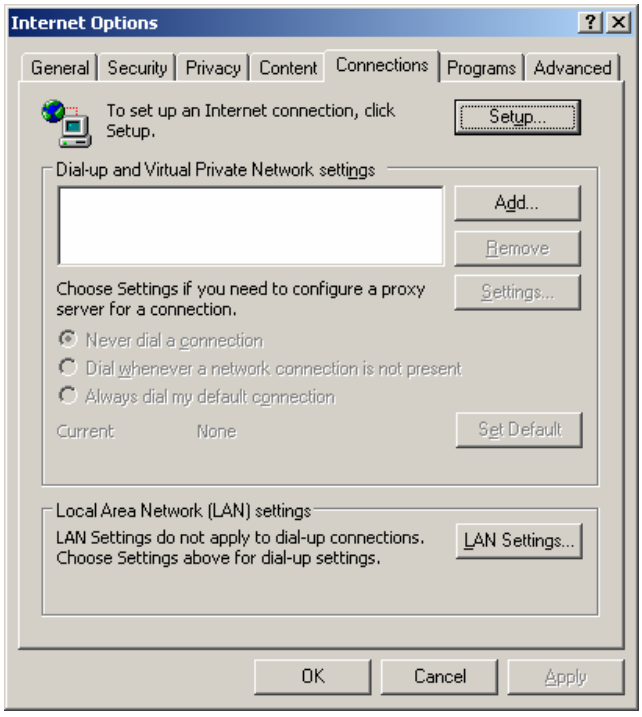
Step 10. Input “**exit**” in the box of Command Prompt, and then press enter.



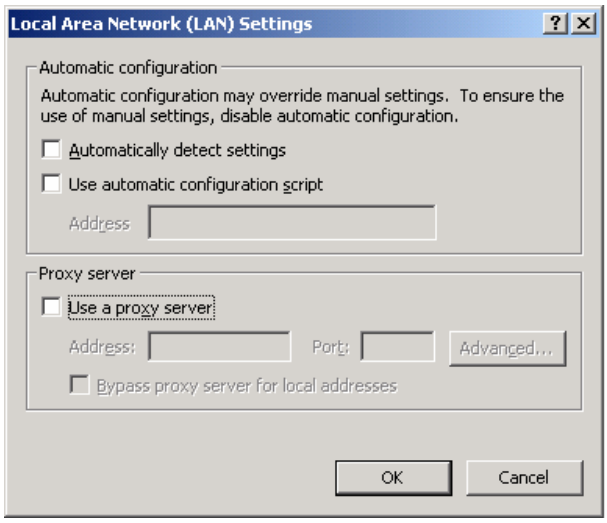
Step 11. Please select “**Internet Options**” under “**Tools**” of your IE Browser.



Step 12. In this dialogue box, please select “**Connections**” in the **“LAN Settings**”.



Step13. Please **DO NOT** tick all of the selection boxes. Press "**OK**" after finishing with the setup.



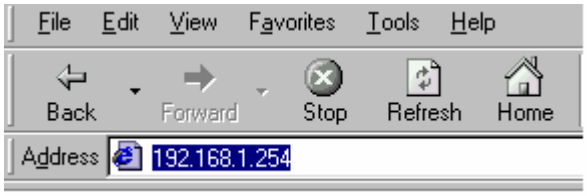
If your ISP Company has a designated Proxy setting, key in the setting after you complete the GN-BR404W configuration.

Now, please jump to Section 3-3 to setup broadband router.

3-3. Setup for Broadband Router

The GN-BR404W provides Web based configuration. You can configure your GN-BR404W through your Internet Explorer browser or Netscape Communicator.

Step 1. Key in the preset IP address“**192.168.1.254**” in the address column in the browser, and then press enter.



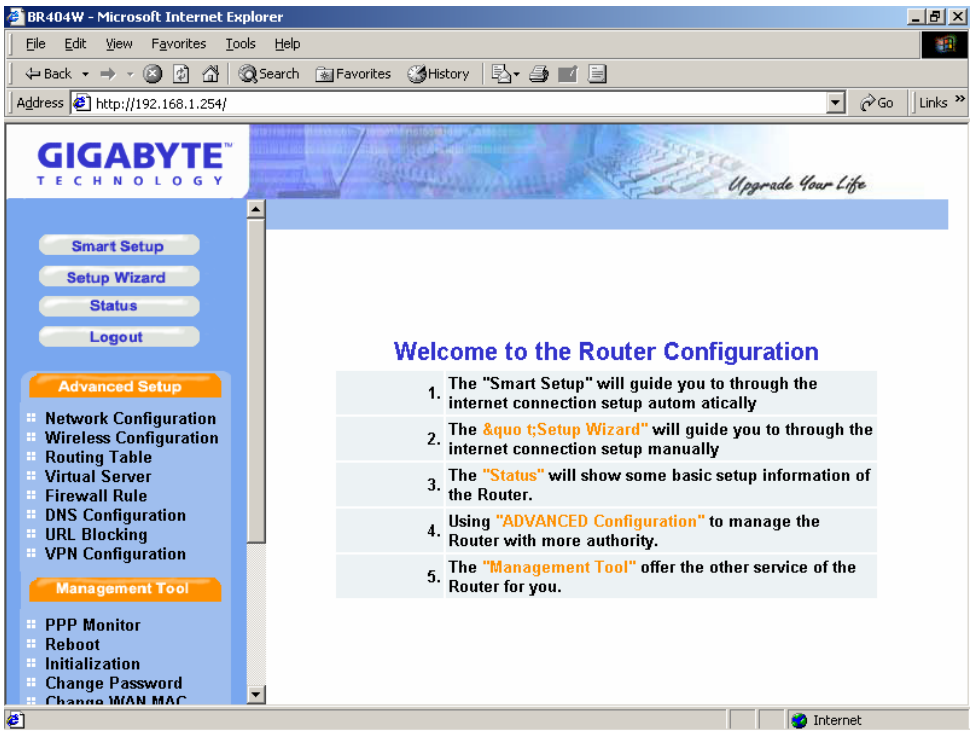
If you have more than one router or IP conflict problem on the same subnet, please follow the IP change priority table shown as below.

priority1	*"192.168.1.254"*	*"255.255.255.0"*	*"192.168.1.1"*	*"192.168.1.33"*
priority2	*"192.168.2.254"*	*"255.255.255.0"*	*"192.168.2.1"*	*"192.168.2.33"*
priority3	*"172.16.1.254"*	*"255.255.255.0"*	*"172.16.1.1"*	*"172.16.1.33"*
priority4	*"172.17.1.254"*	*"255.255.255.0"*	*"172.17.1.1"*	*"172.17.1.33"*
priority5	*"10.1.1.254"*	*"255.255.255.0"*	*"10.1.1.1"*	*"10.1.1.33"*
priority6	*"10.2.1.254"*	*"255.255.255.0"*	*"10.2.1.1"*	*"10.2.1.33"*

Step 2. The dialogue box will appear as shown in the following diagram, and key in the default user name “**admin**” for the wideband network GN-BR404W and the default password “**admin**”, and then press “**OK**”.

Step 3. The homepage of the GN-BR404W will appear as shown below. If you are the first time to configure the router and you have connected to the WAN port, the system will detect your wan type automatically through the “**Smart Setup**” function. Please refer to the instruction of the “**Smart Setup**”.

If you want to configure the wan type manually, you can click the “**Setup Wizard**” on the screen, and such Setup Wizard will guide you to complete the necessary steps for the setup on screen as follows.

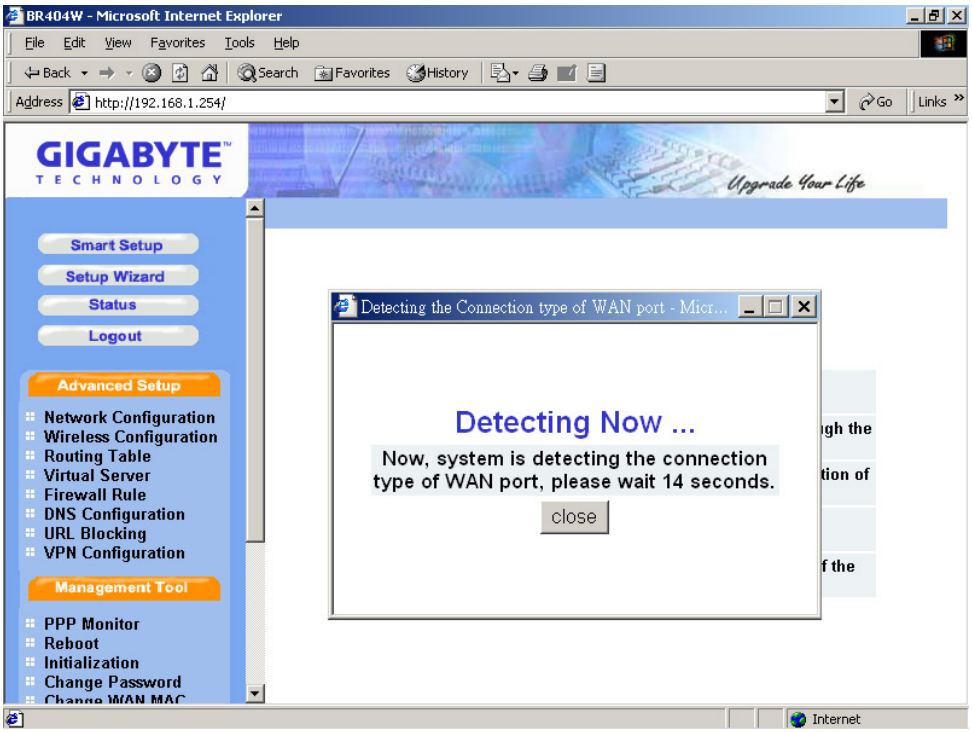


Smart Setup

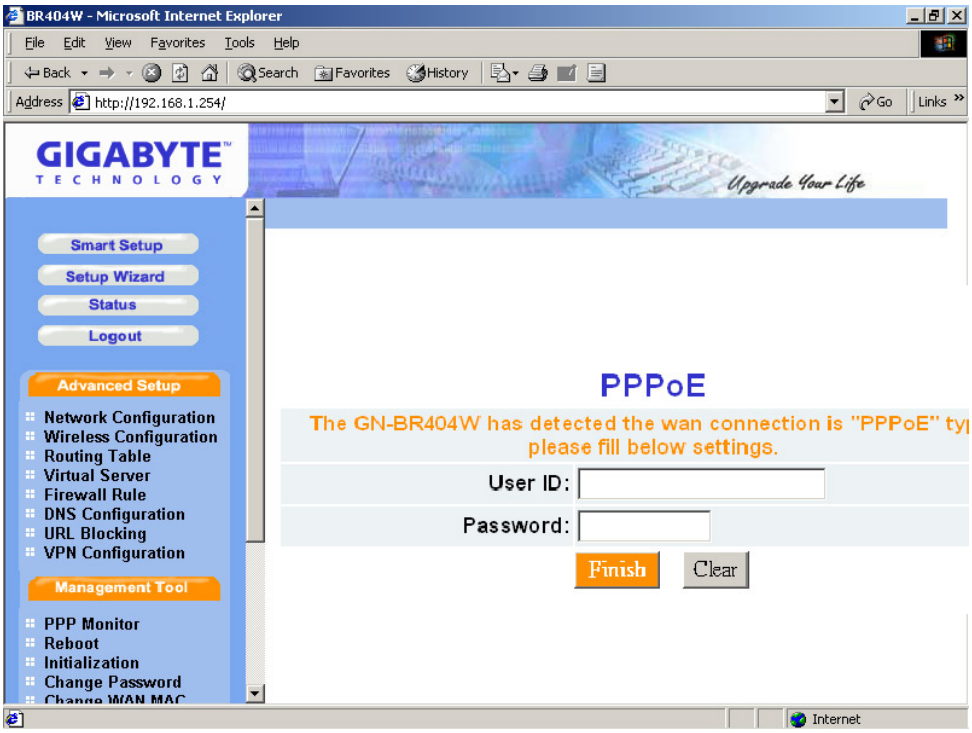
If you are the first time to configure the router and you have connected to the WAN port, the "**Smart Setup**" function can detect your wan type automatically through the Internet connection. And it will guide you to complete the wan setting step by step.

System automatic detection:

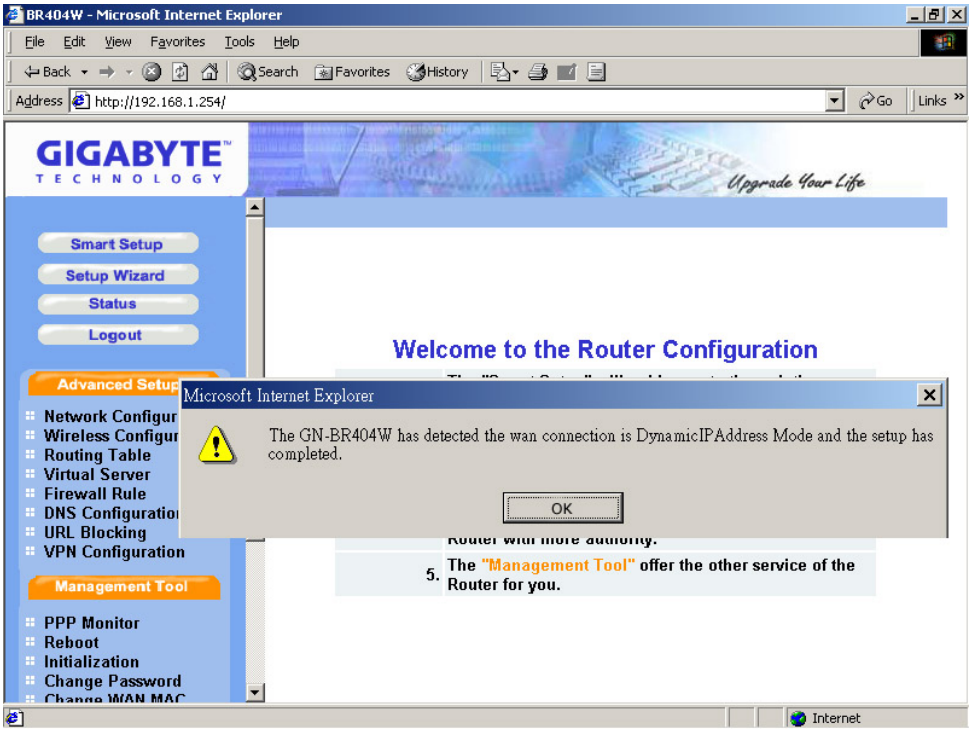
Step1. The system is detecting the WAN connection type, and will show the detective result later.



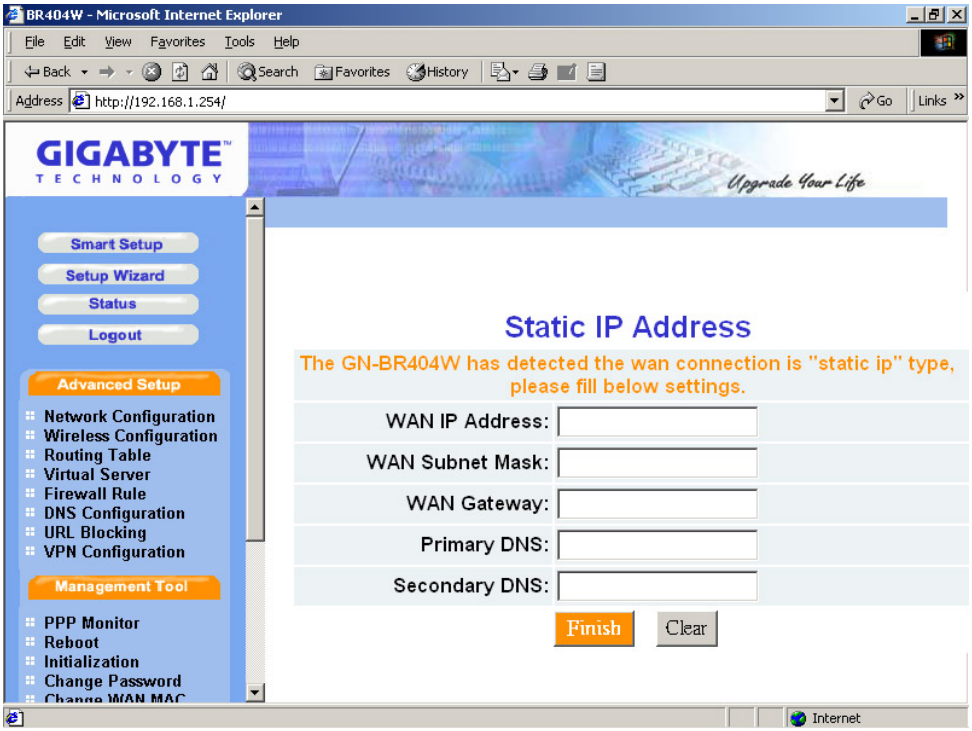
Step2. If you are the **PPPoE user**, the screen will appear as shown below. Please enter the User ID and Password information that your ISP provided you.



Step3. If you are the **dynamic IP address user**, the device will save the configuration and there is no necessary to reboot the device. Please click “OK” button.

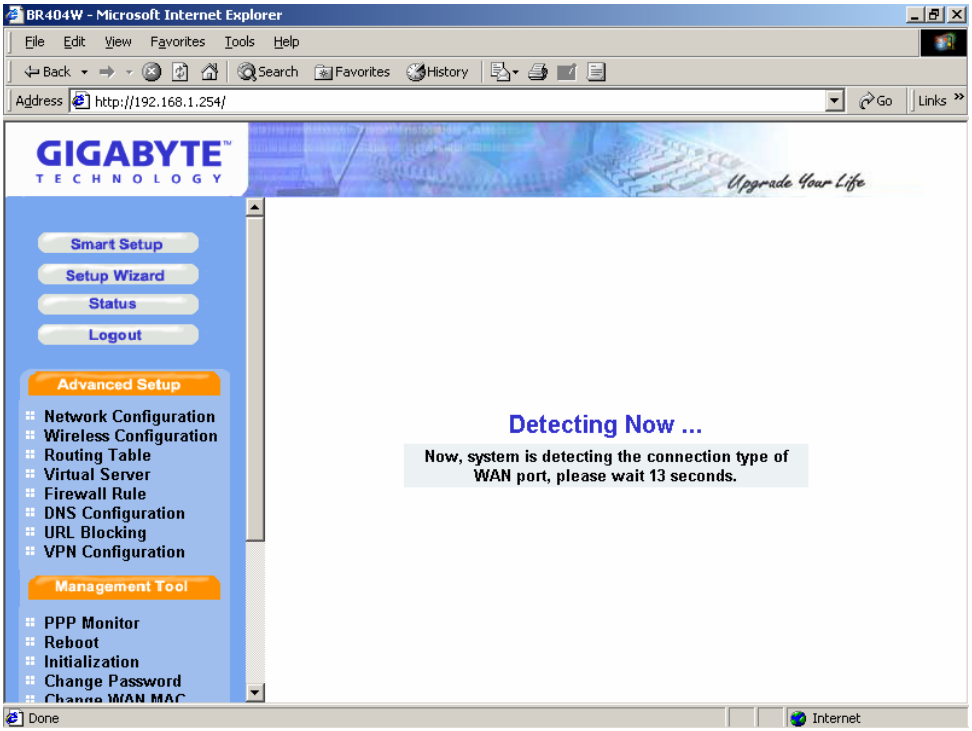


Step4. If you are the Static IP address user, the screen will appear as shown below. Please enter the WAN IP address, WAN subnet mask, WAN gateway, and DNS information that your ISP provide you.

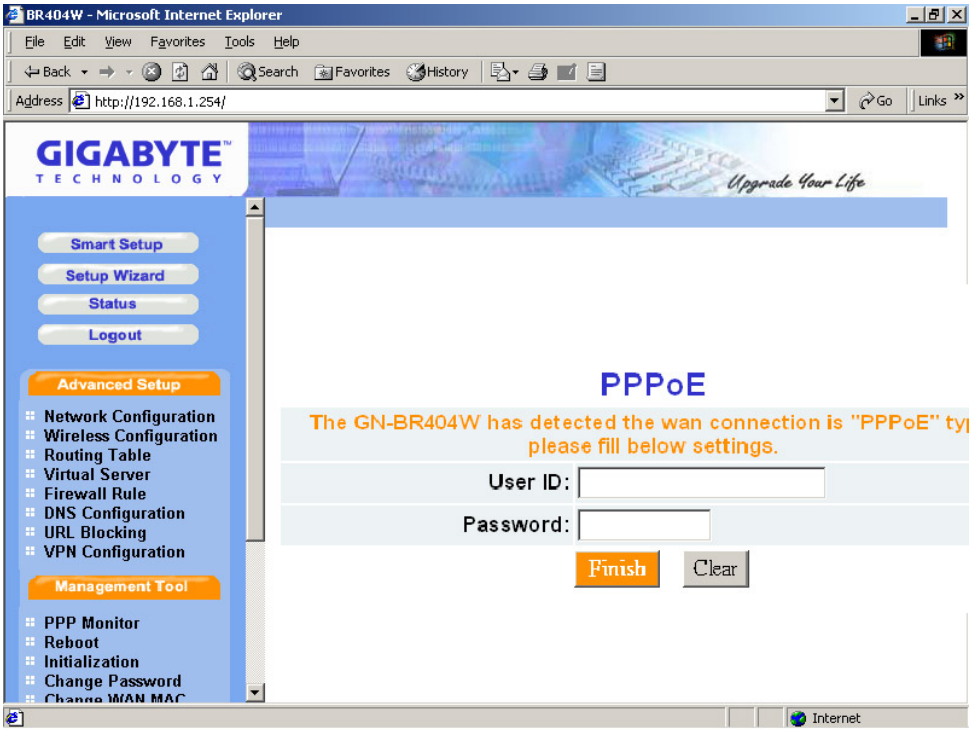


Click Smart Setup manually:

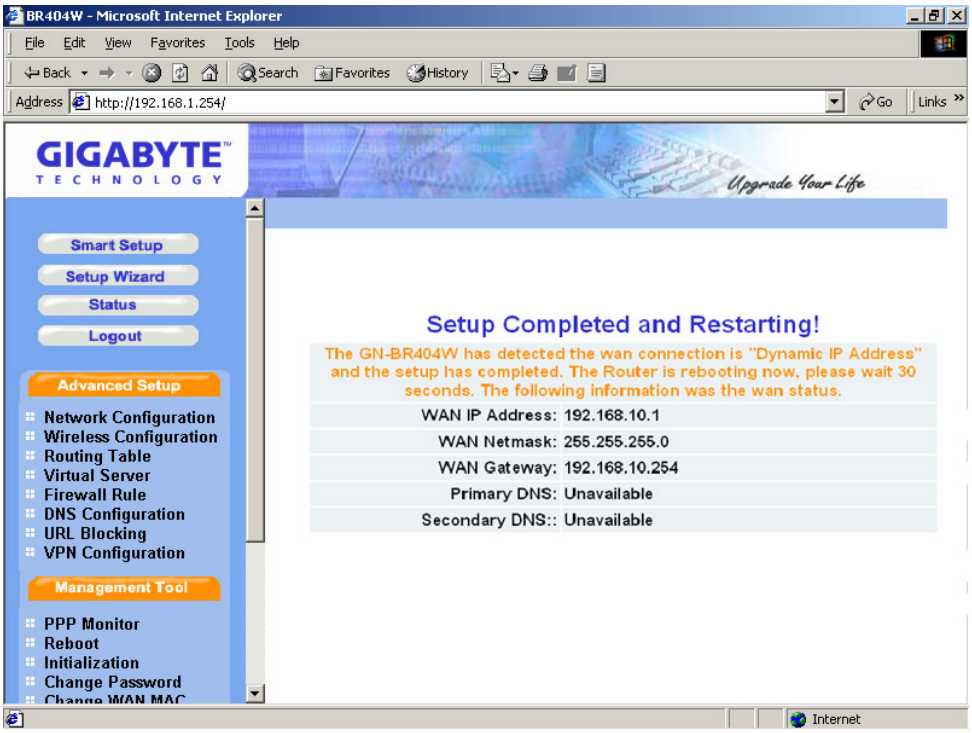
Step 1. The system is detecting the WAN connection type, and will show the detective result later.



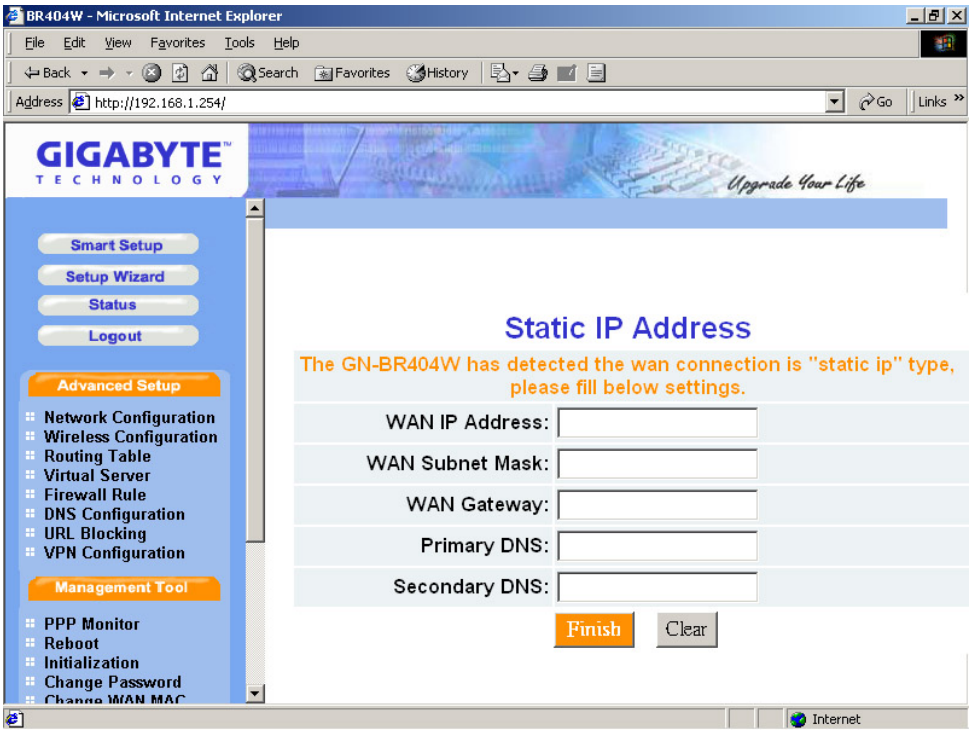
Step2. If you are the **PPPoE user**, the screen will appear as shown below. Please enter the User ID and Password information that your ISP provided you.



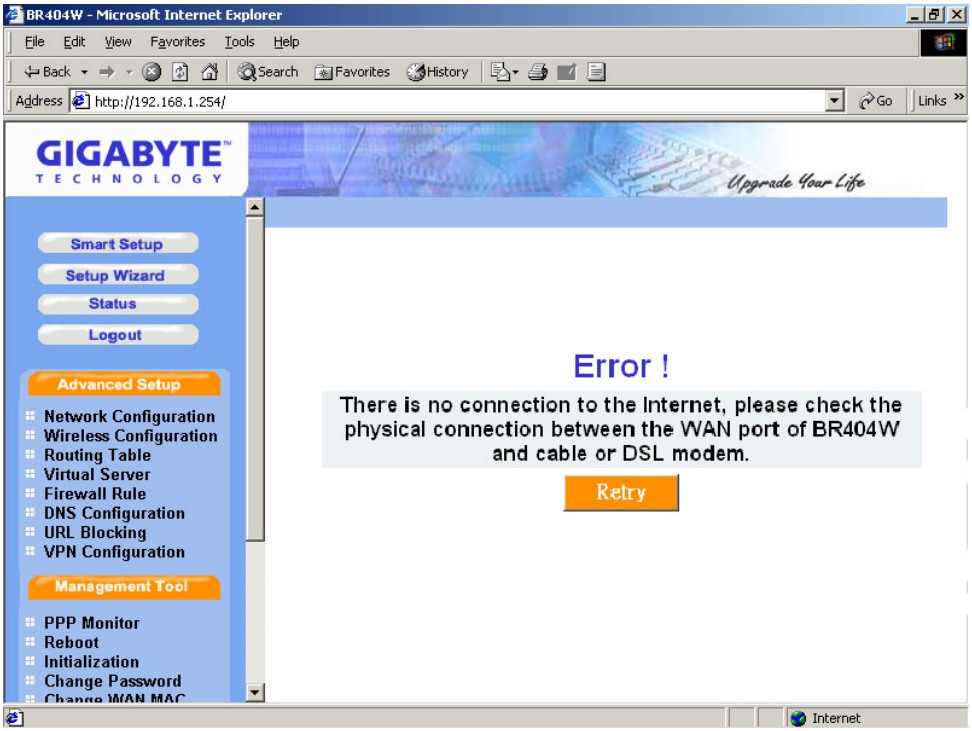
Step3. If you are the **dynamic IP address user**, the device will save the configuration and there is no necessary to reboot the device.



Step4. If you are the Static IP address user, the screen will appear as shown below. Please enter the WAN IP address, WAN subnet mask, WAN gateway, and DNS information that your ISP provide you.



Note: *If the device can not detect the WAN Ethernet link signal, it will show the error message. Please check the physical connection between GN-BR404W and cable or DSL modem.*



Setup Wizard

Step1. "**LAN Setup**" is shown in the diagram. *Each setup item of the local area network is default setting, and is not necessary to make change to it* for normal operation. Please input the settings on your own if change is needed.

DHCP Setup:

- "**enable**" indicates that the DHCP function of the GN-BR404W is initialized, and you configure the computers on your network to "Obtain an IP address automatically", then when you turn your computer "On", it will automatically load the proper TCP/IP setting from GN-BR404W. (Configure the DHCP starting address and the DHCP allocation number on your own.)

- "**disable**" indicates that it will not automatically load proper TCP/IP setting from the GN-BR404W. You will have to configure all the TCP/IP setting for your network manually. (It is not necessary to configure the DHCP starting address and the DHCP allocation number.)

DHCP Start Address / End Address :

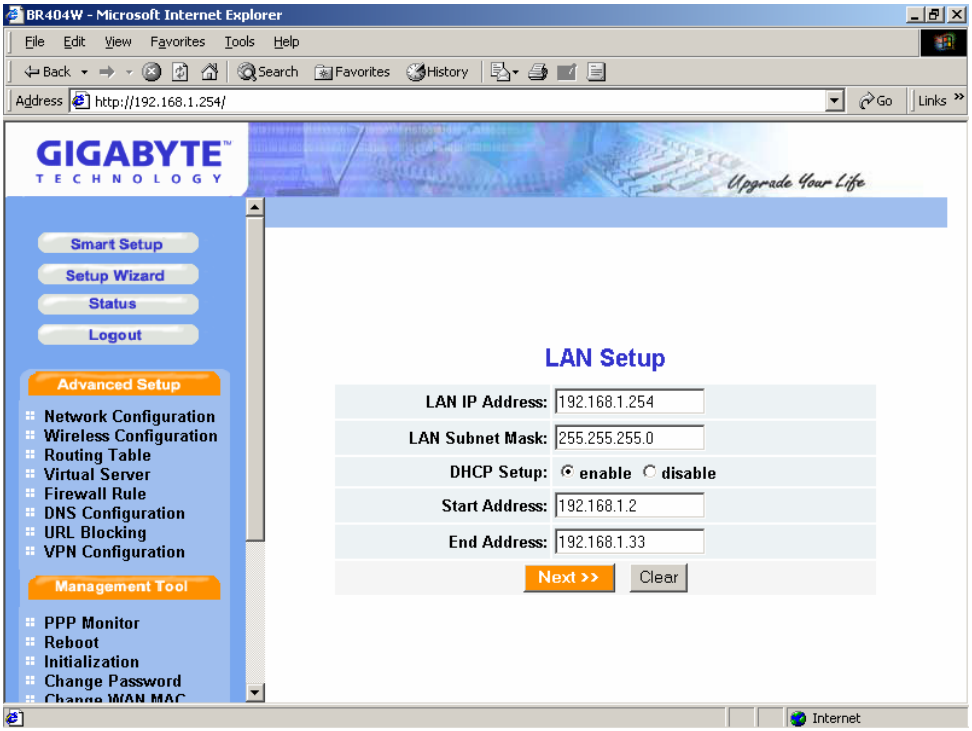
When the DHCP setting is "enable", the GN-BR404W uses this allocable range of the IP address as the initial value to assign the IP to the PC connected to the LAN end.

For example:

The DHCP start address is 192.168.1.1 and the end address is 192.168.1.50 .
The IP allocable range of the DHCP is from 192.168.1.1 to 192.168.1.50.

The LAN IP address "192.168.1.254" is the default IP address of the GN-BR404W.

Click "**Next**", and the following screen will appear:



Step 2. Choose your desired wide area network mode.

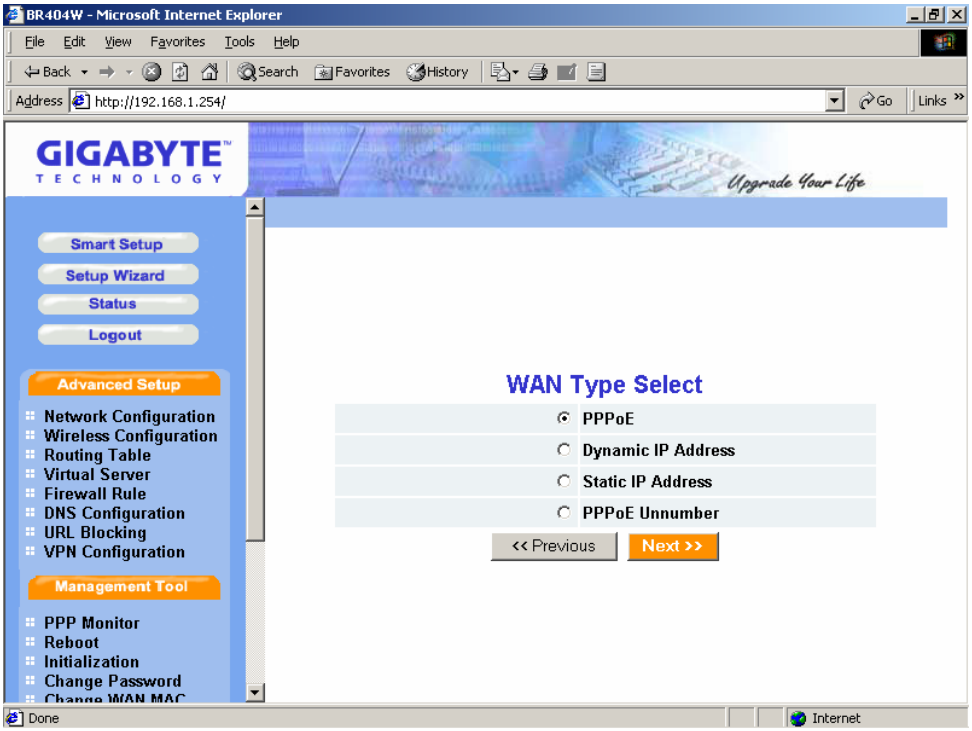
- "**PPPoE**"**:** If you are using the hourly rate for the ADSL, please select this item. And then please follow Step 3

- "**Dynamic IP Address**"**:** If you use the wideband fixed connection of ADSL/Cable Modem, but do not have a static IP, please select this item. And then please follow Step 7

- "**Static IP Address**"**:** If you use the wideband fixed connection of ADSL/Cable Modem, but have a static IP, please select this item. And then please follow Step 11

- "**PPPoE Unnumber**": If you are the user of the PPPoE Unnumber, please select this item. And then please follow Step15.

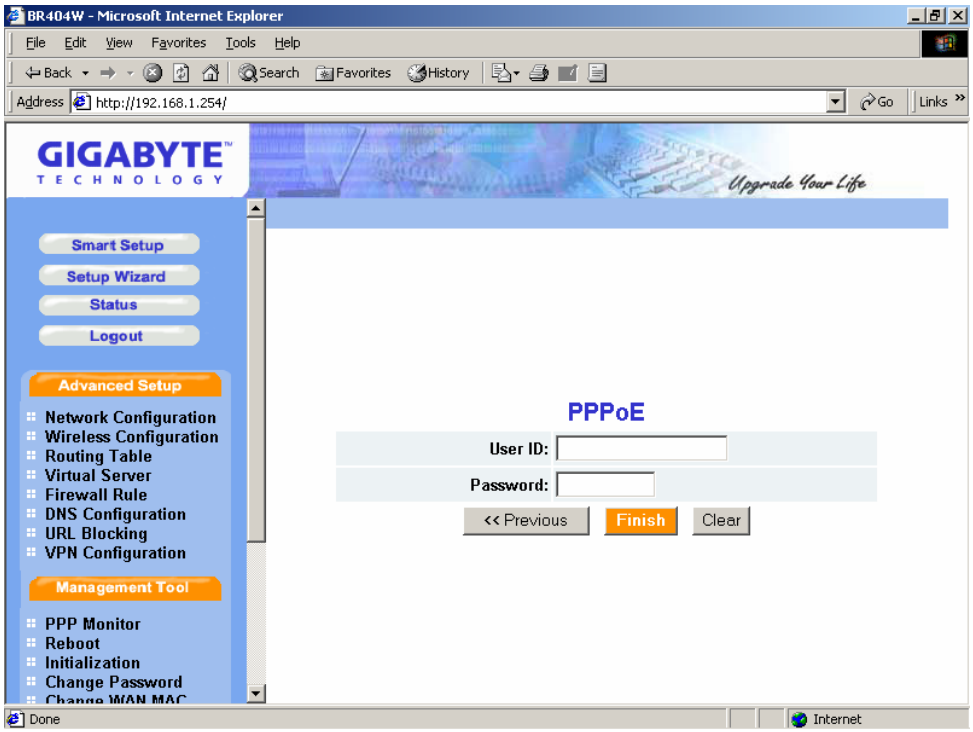
After your desired wide area network mode is selected, please press "**Next**".



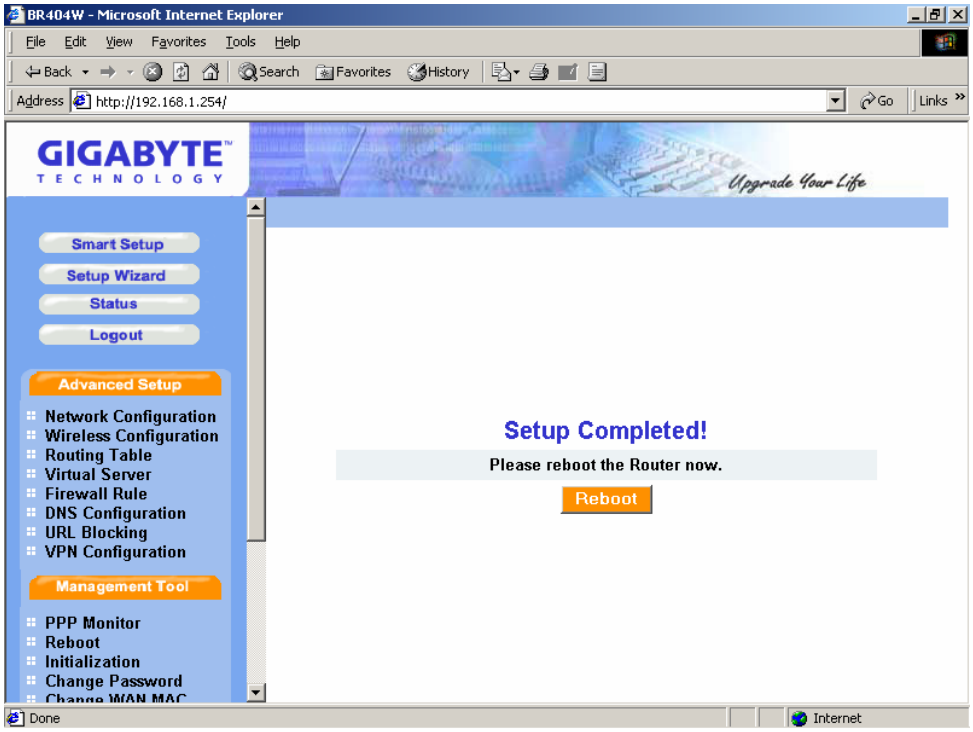
Step 3. If you select "**PPPoE**" under the WAN TYPE SELECT, key in the User ID and password. The wideband company provides the above data, and press "**Finish**" to go to next step.

PPPoE User ID and Password:

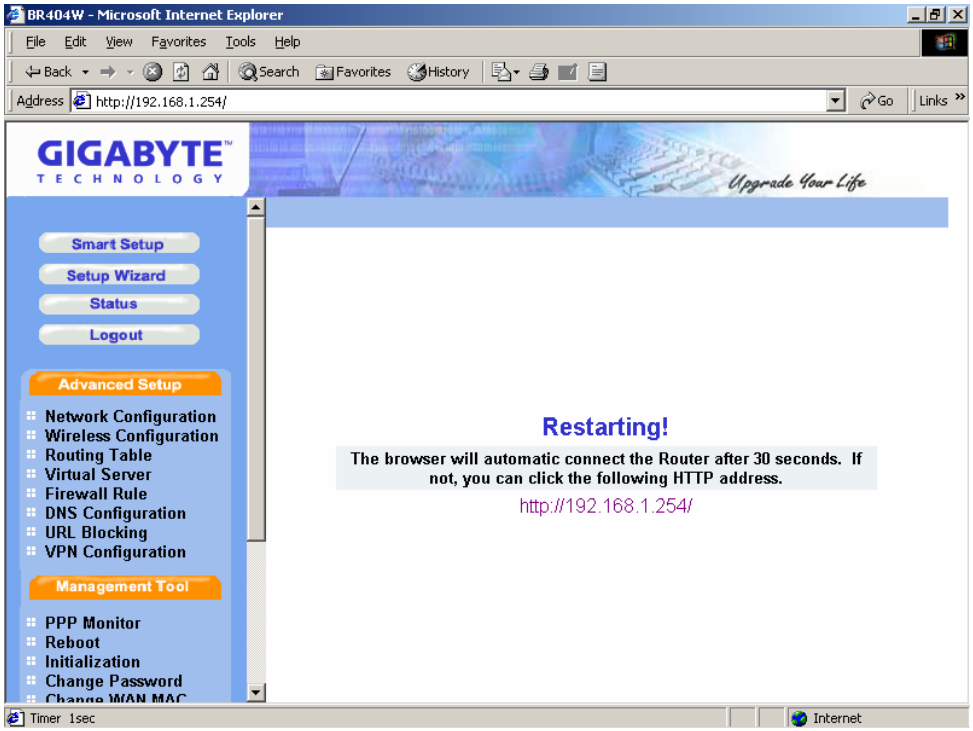
The "User ID" and "Password" are your ISP assigned to you.



Step 4. Press “**Reboot**” to go to next step.

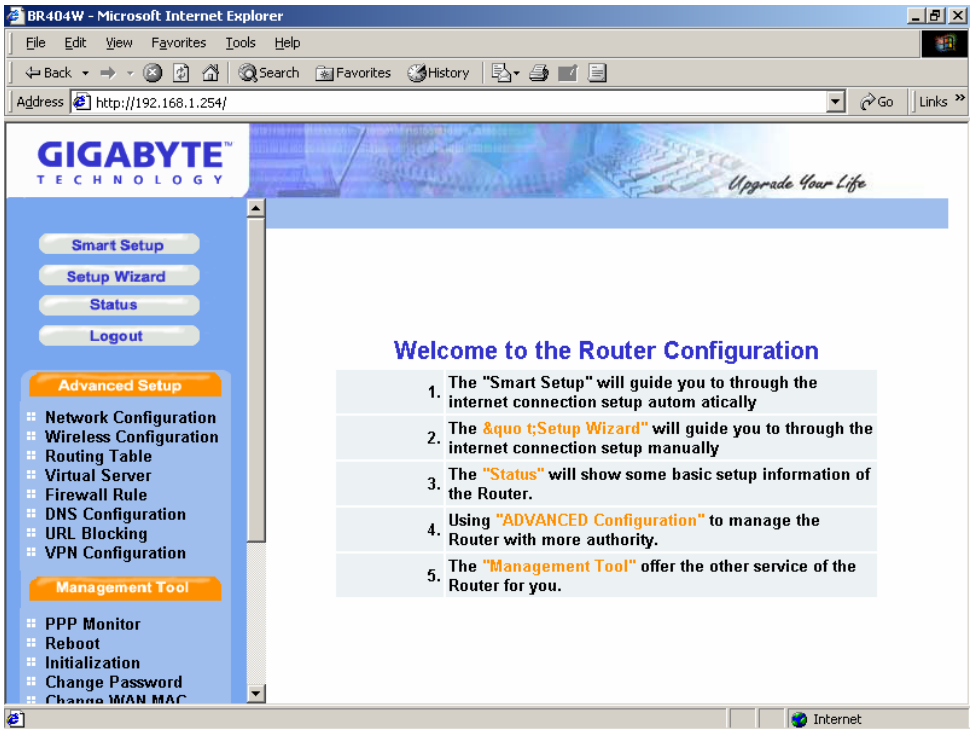


Step 5. Please wait a moment.

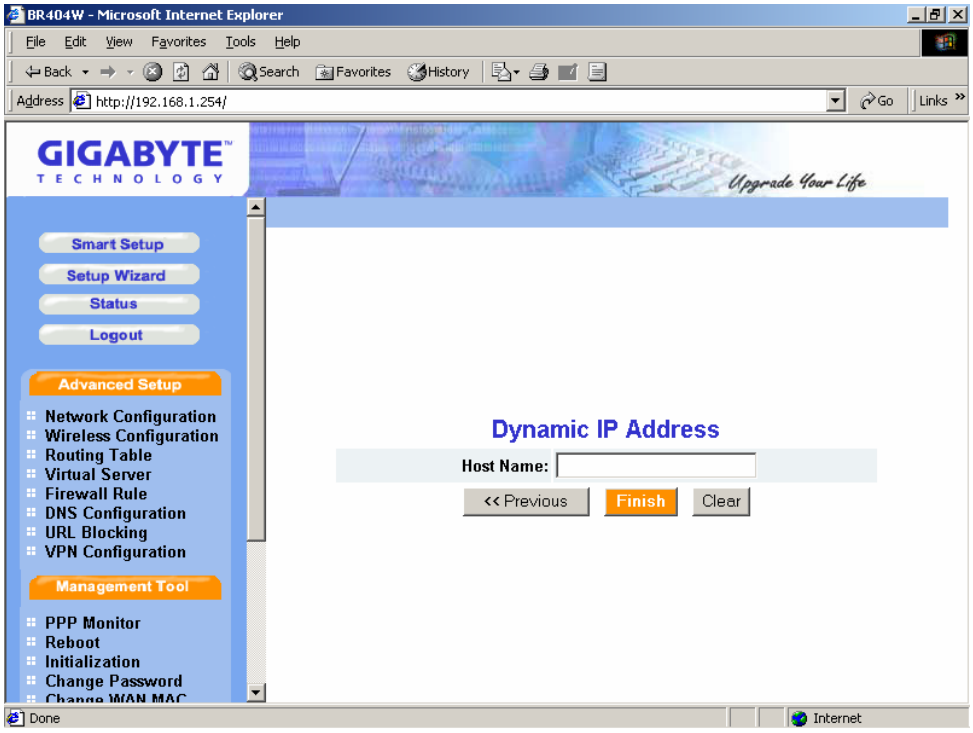


Step 6. The IE browser will be automatically connected to the main menu, and your setup has completed by then. Please use your IE connect to Internet.

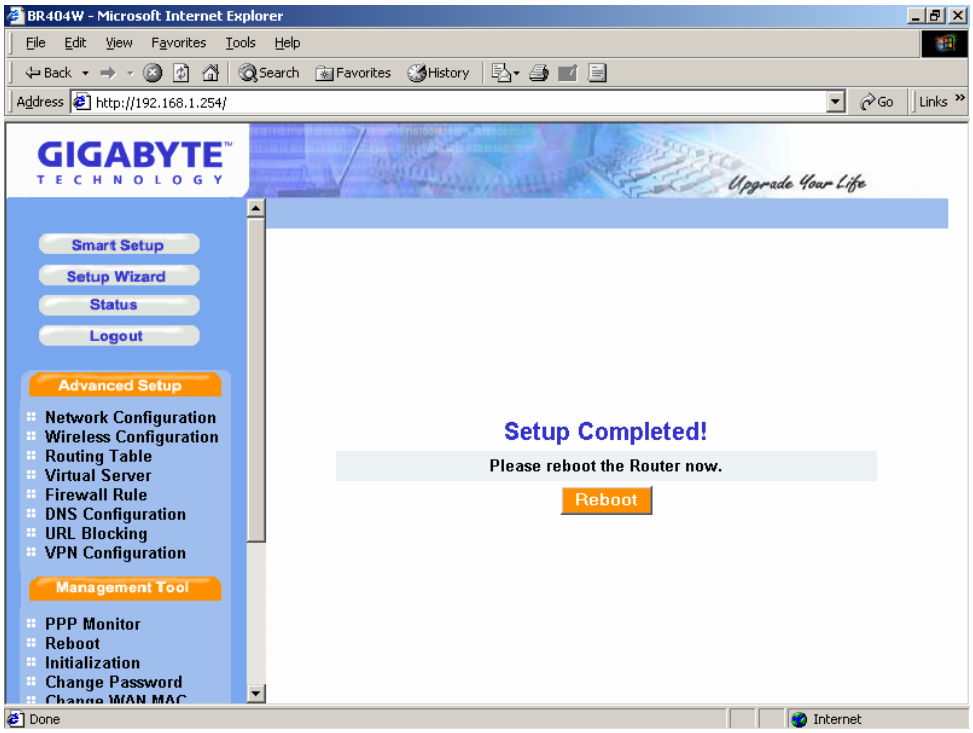
If you can connect to the Internet , the setting is completed. If you use the Wireless Lan Card connection or need further setting, please continue to section 3-4 Advanced Setup.



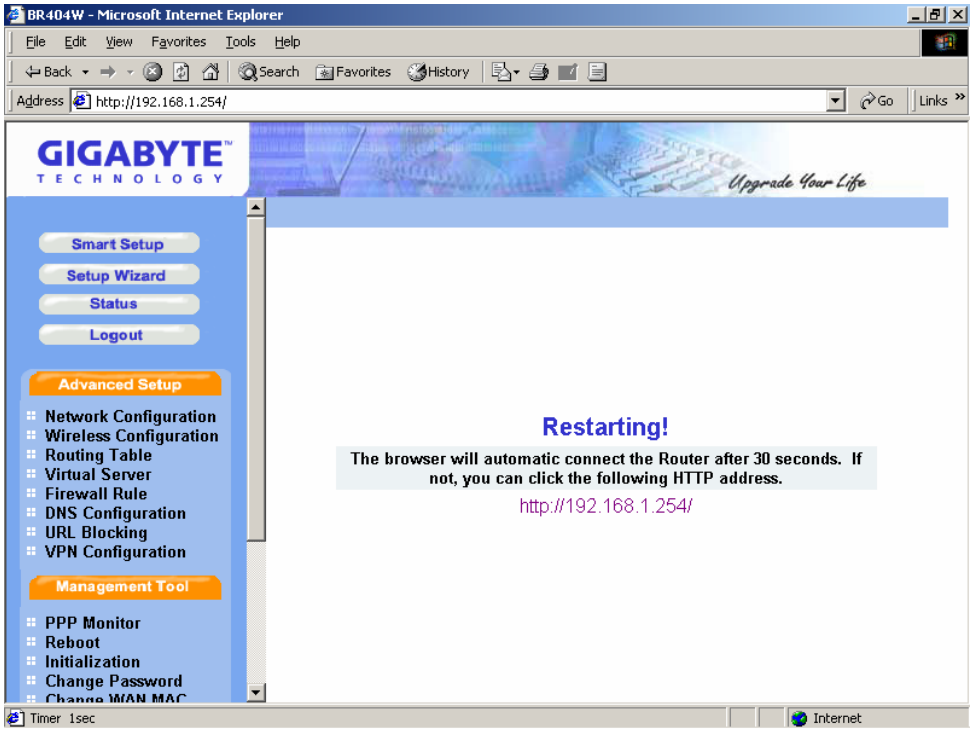
Step 7. If you select the "**Dynamic IP Address**" in the WAN TYPE SELECT, the following screen will appear. Please key in the Host Name if your ISP has provided. And then press "**Finish**" to go to next step.



Step 8. Press "**Reboot**" to go to next step.

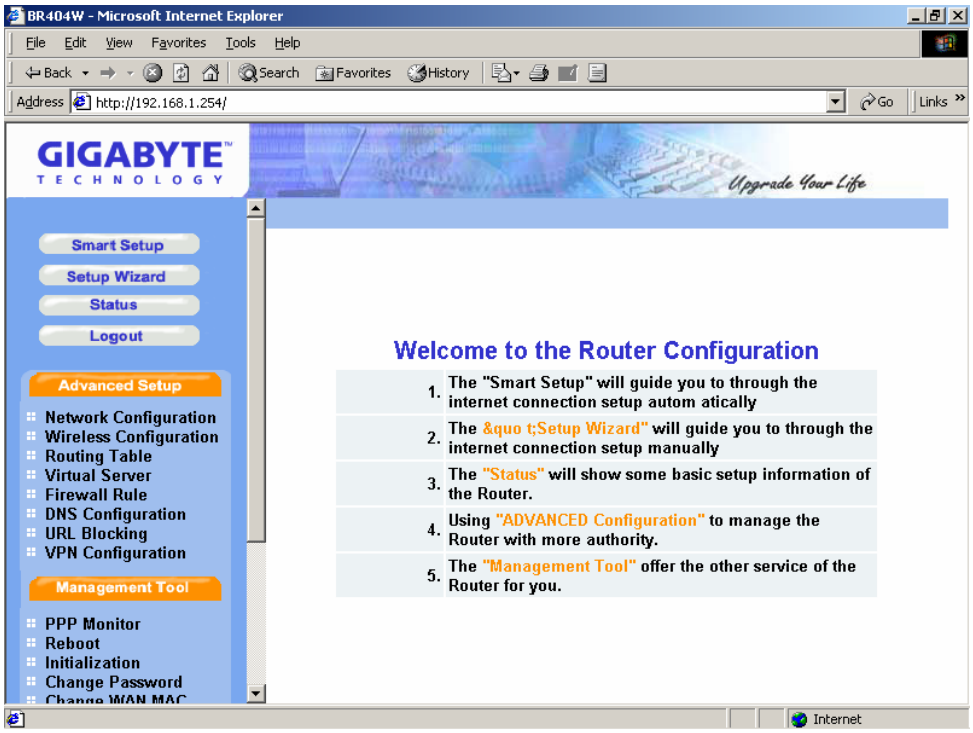


Step 9. Please wait a moment.



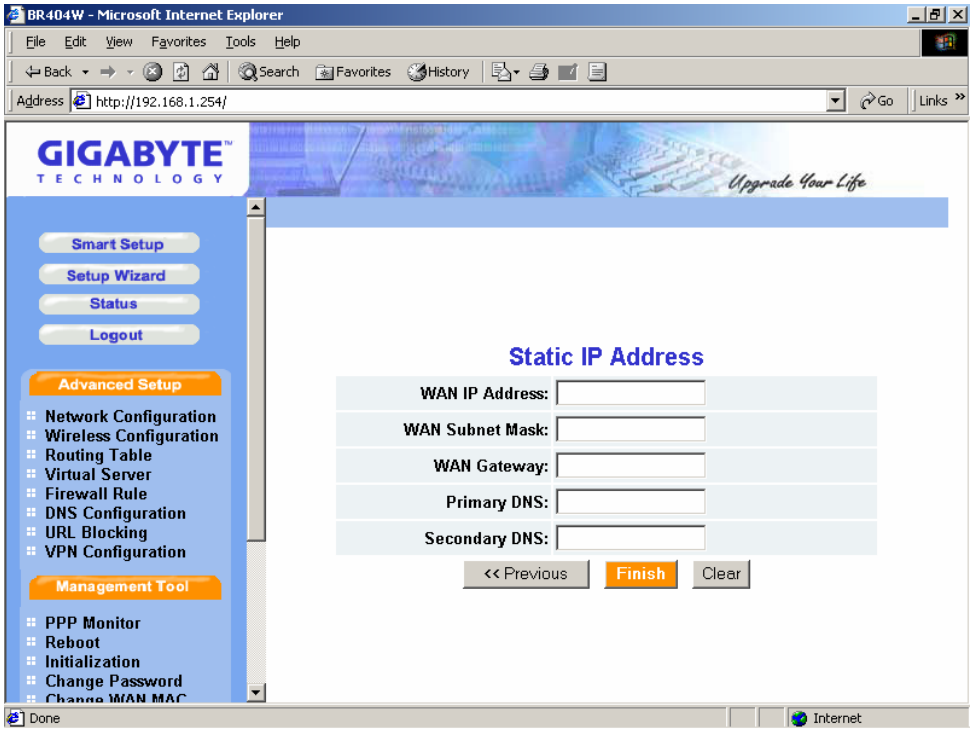
Step 10. The IE browser will be automatically connected to the main menu, and your setup has completed by then. Please use your IE connect to Internet.

If you can connect to the Internet , the setting is completed. If you use the Wireless Lan Card connection or need further setting, please continue to section 3-4 Advanced Setup.

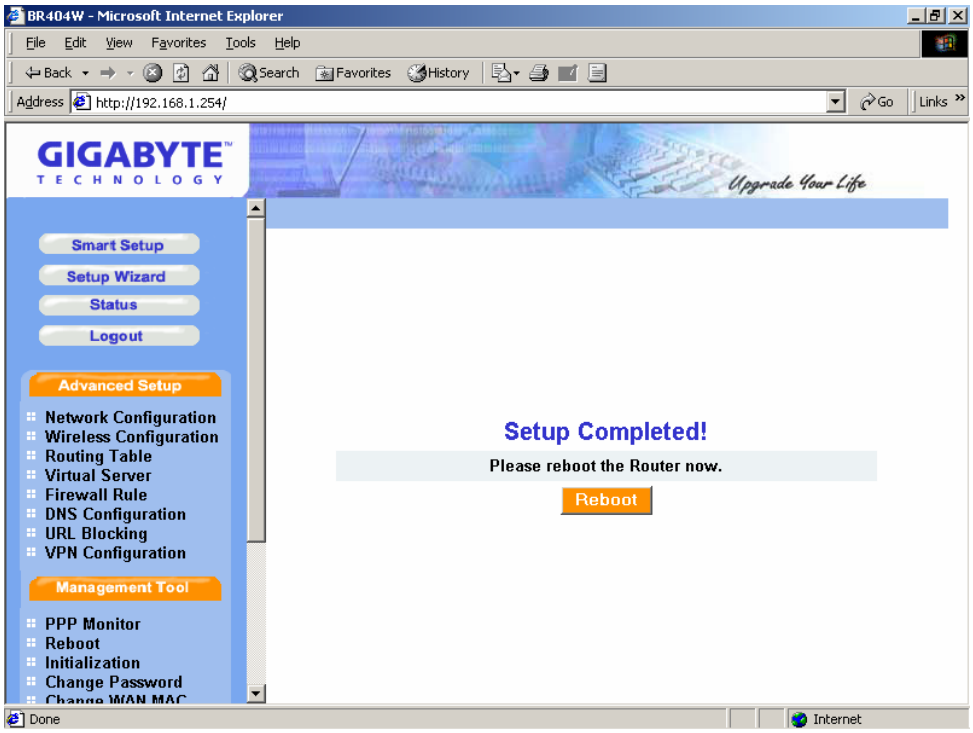


Step 11. If you select “**Static IP Address**” in the WAN TYPE SELECT, please key in the data provided by the wideband company in the following fields as shown below. And then press “**Finish**” to go to next step.

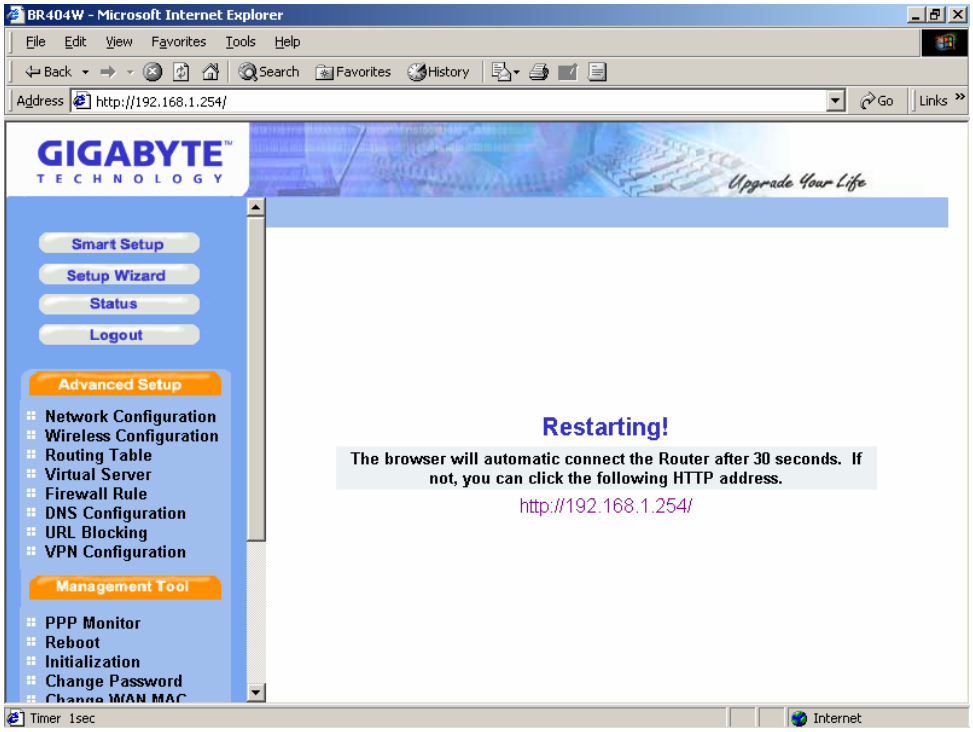
If your wideband company gives you more than one IP address, then select one of them to fill in the column in the following fields.



Step 12. Press “**Reboot**” to go to next step.

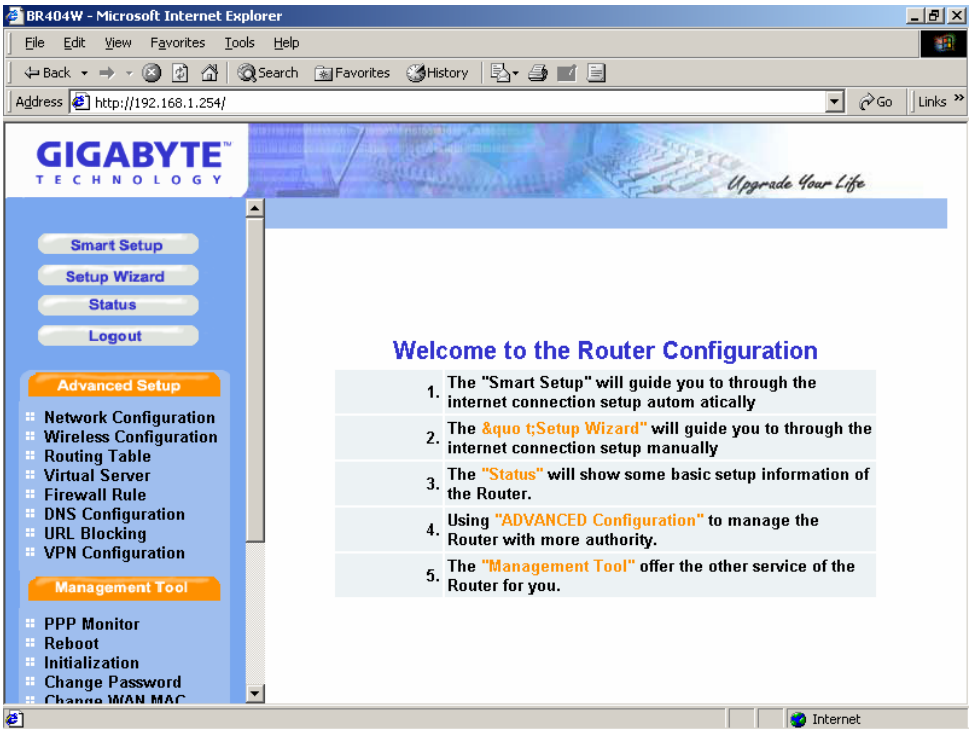


Step 13. Please wait a moment.



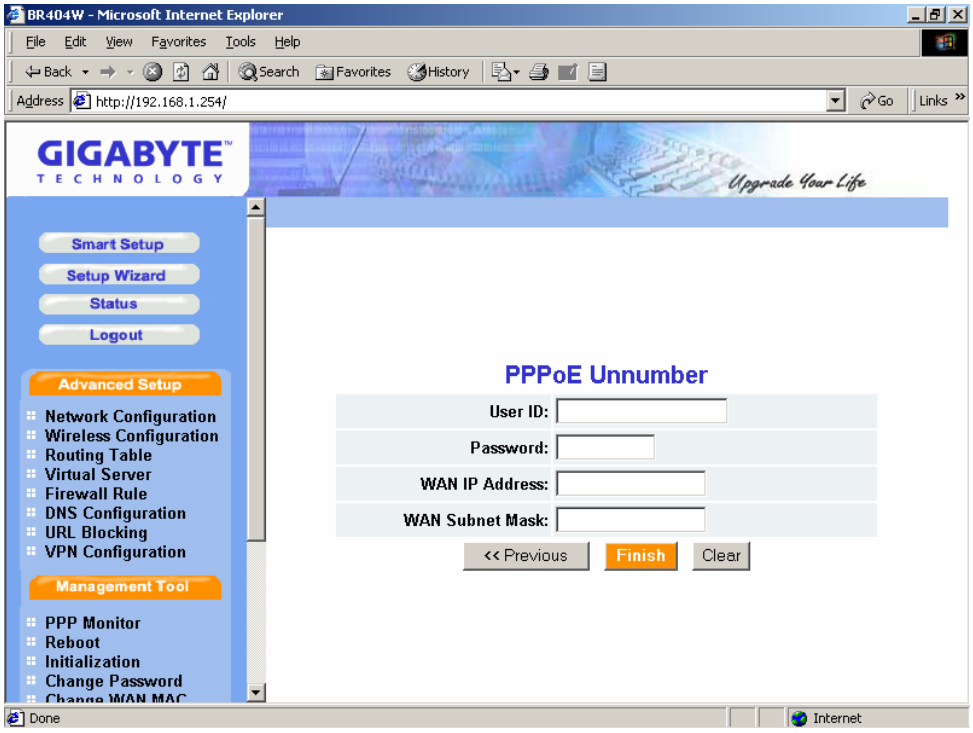
Step 14. The IE browser will be automatically connected to the main menu, and your setup has completed by then. Please use your IE connect to Internet.

If you can connect to the Internet , the setting is completed. If you use the Wireless Lan Card connection or need further setting, please continue to section 3-4 Advanced Setup.

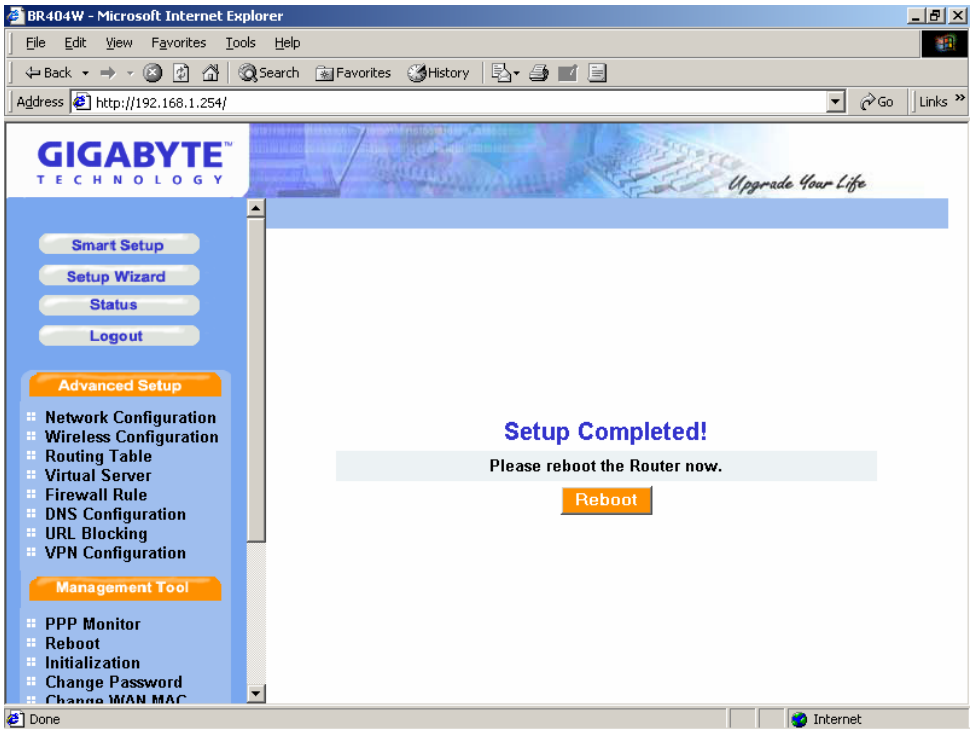


Step 15. If you select “**PPPoE Unnumber**” in the WAN TYPE SELECT, please key in the data provided by the wideband company in the following fields as shown below. And then press “**Finish**” to go to next step.

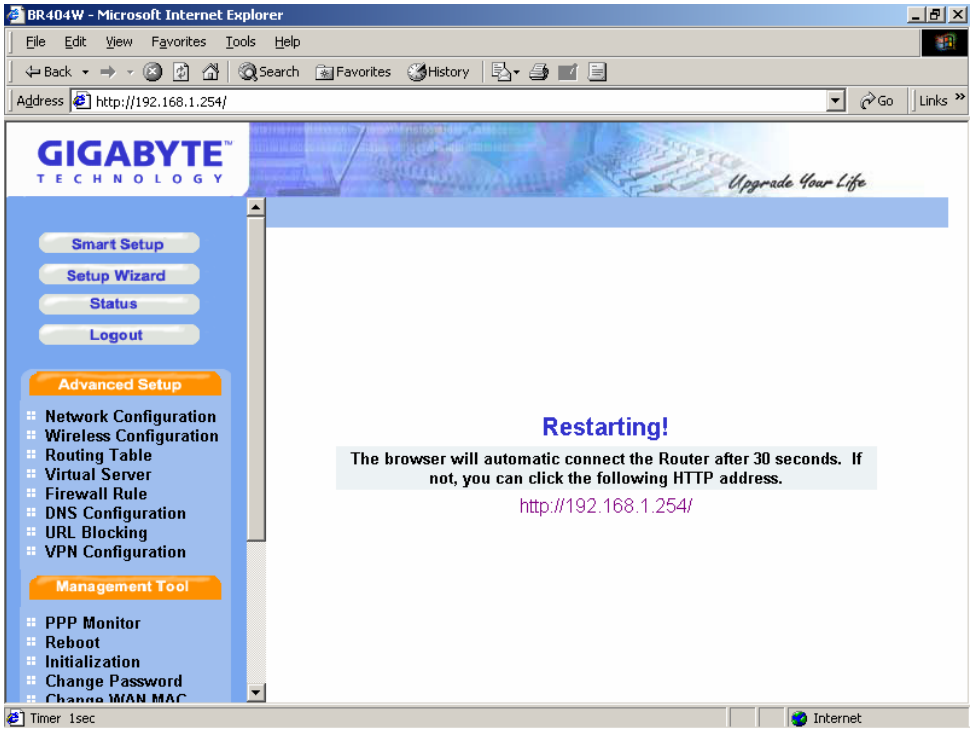
If your wideband company gives you more than one IP address, then select one of them to fill in the column in the following fields.



Step 16. Press “**Reboot**” to go to next step.

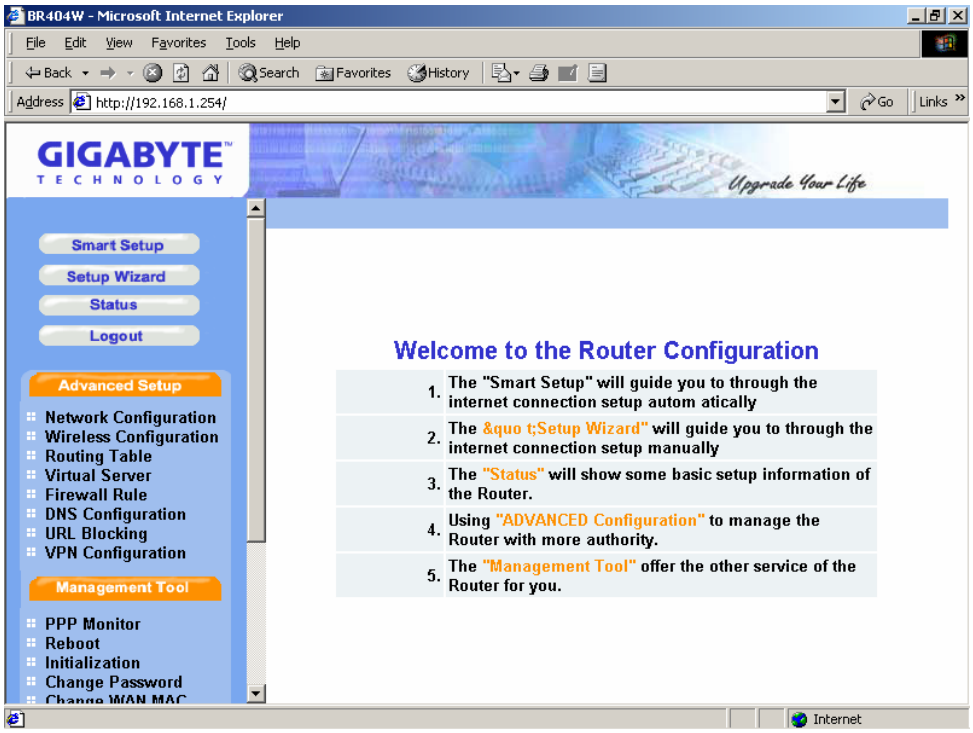


Step 17. Please wait a moment.



Step 18. The IE browser will be automatically connected to the main menu, and your setup has completed by then. Please use your IE connect to Internet.

If you can connect to the Internet , the setting is completed. If you use the Wireless Lan Card connection or need further setting, please continue to section 3-4 Advanced Setup.



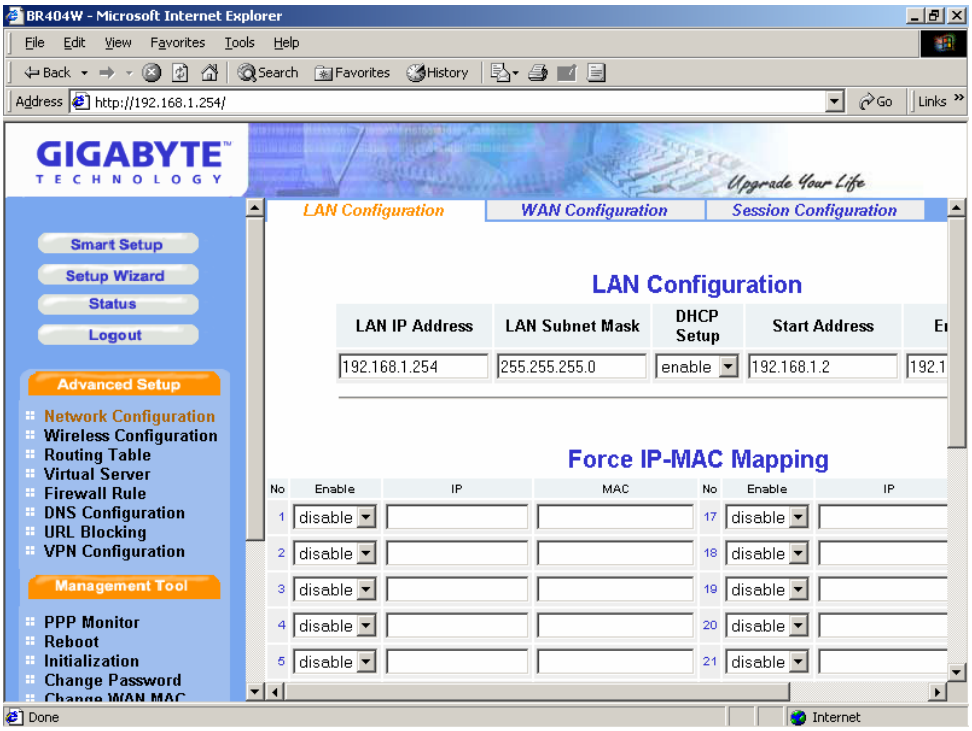
3-4. Advanced Setup

This section will show you the advanced setup of the GN-BR404W if you need require special configuration.

3-4-1. Network Configuration

The Network Configuration function allows you to access to the LAN Configuration, WAN Confguration and Multisession Configuration.

- **LAN Configuration**



◈ ***LAN Configuration***

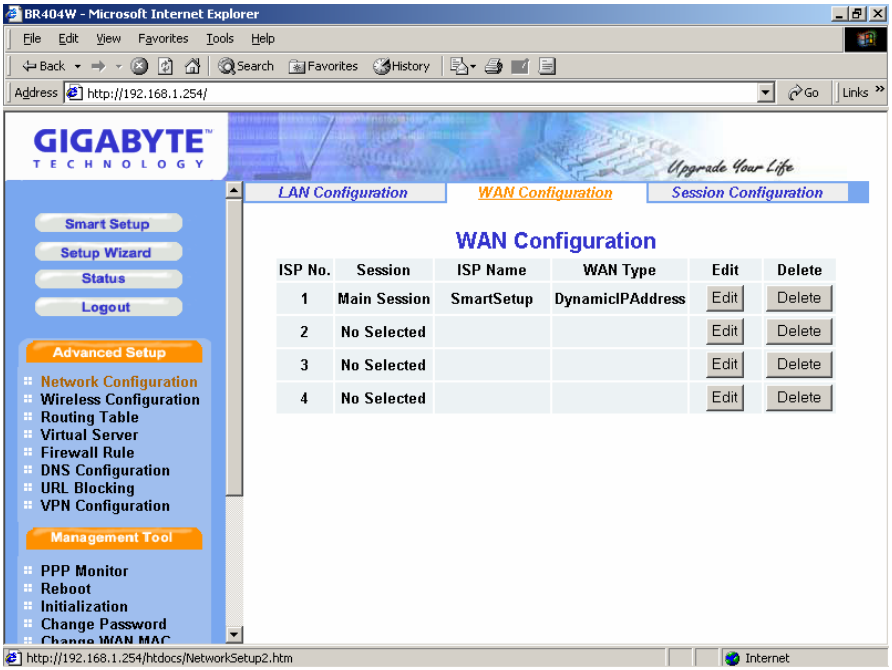
From this table, you can modify the LAN setting if it necessary.

◈ ***Force IP-MAC Mapping***

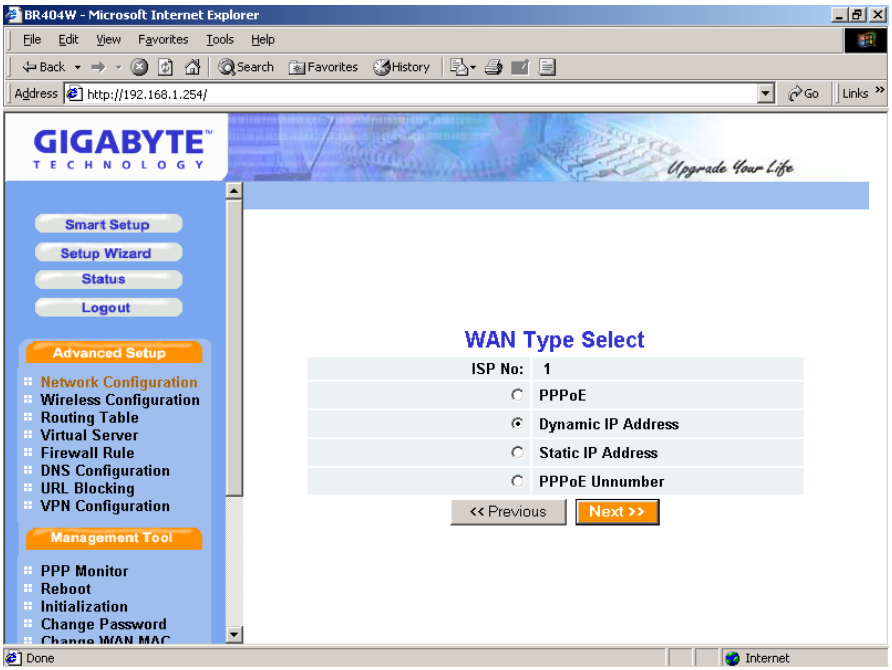
This Function allows you to assign a specific IP address to one specific PC.

Verify the desired setting and then click the "**Submit**" button to set the value into GN-BR404W.

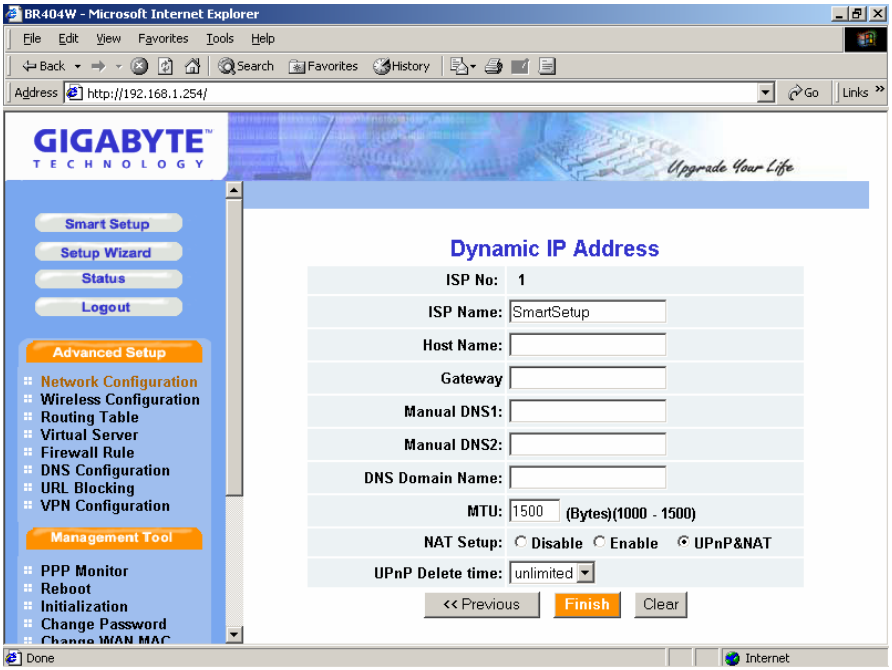
■ WAN Configuration



This page is the further configuration of the WAN connection. You can setup up to 4 WAN connection entries. Each entry may has it's own connection type (PPPoE, PPPoE Unnumber, Dynamic IP address, Static IP address) and some other properties. For example, when you click the "**Edit**" button of the ISP No.1 (WAN Type: Dynamic IP Address) on the table then there will appear the screen as follows.



Click "**Next**".



◈ ***ISP Name, Host Name, Gateway, DNS1 and DNS2 Address, DNS Domain Name***

Those information are provided by your ISP company.

◈ ***MTU(Maximum Transmission Unit)***

This defines the maximum size of the packets sent from your computer onto the network. Any messages larger than the MTU are divided into smaller packets before being sent. Leave this on the default value(1500) unless you have a particular reason to change it.

◈ ***NAT Setup***

The Internet is expanding at an exponential rate. As the amount of information and resources increases, it is becoming a requirement for even the smallest businesses and homes to connect to the Internet. Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. This allows home users and small businesses to connect their network to the Internet cheaply and efficiently.

Universal Plug and Play (UPnP) is an architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these devices to automatically connect with one another and work together to make networking - particularly home networking

- possible for more people.

Normal user please select “**NAT enable**” or “**UPnP&NAT**” then connect to the Internet in general.

◈ ***UPnP Delete Time***

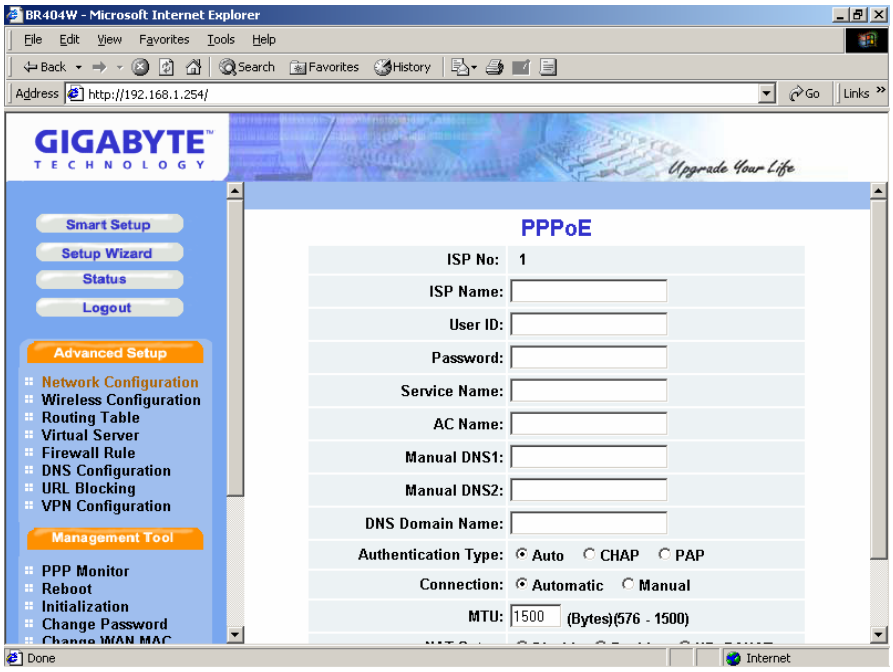
This variable determines the time to live in hours of a port-mapping lease when the value of Lease Time is 0.

Note: *If the WAN IP address which got form a DHCP server and the LAN IP address are on the same subnet, the LAN IP address will be changed to another subnet automatically and reboot the device.*

Verify the desired setting and then click the “**Finish**” button to set the value into GN-BR404W.

Other WAN Type of the WAN configuration:

PPPoE



◈ ***ISP Name, User ID, Password, Service Name, AC Name, DNS1 and DNS2 Address, DNS Domain Name***

Those information are provided by your ISP company.

◈ ***Authentication Type***

You may choose between “**Auto**”, “**CHAP**” and “**PAP**”. The default is set to “**Auto**”.

Challenge Handshake Authentication Protocol(CHAP). This is the preferred method of authentication for PPP dialup links. With CHAP, the server sends a challenge to which the remote router sends an encrypted reply containing a secret key.

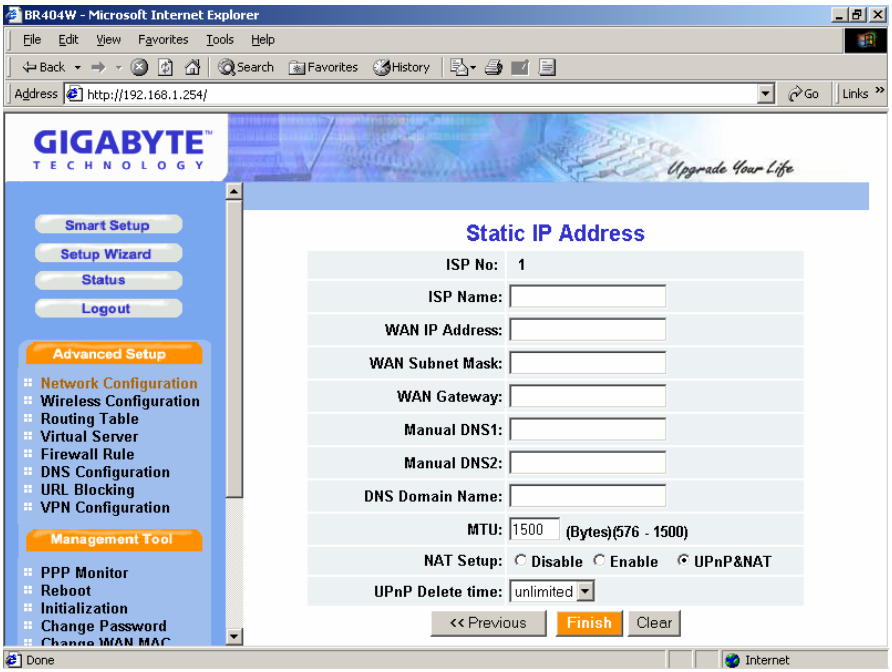
Password Authentication Protocol(PAP) is a simple authentication protocol for PPP allowing a router to identify itself with another router by sending a simple name and password combination. PAP is defined in RFC1334.

◈ ***Connection***

“Automatic” It connects to an ISP without delay when the router is turned on. If connection is disconnected by something troubles, connection have to retry to connect automatically.

“Manual” It connects to an ISP when user presses the “connection” button. If connection is disconnected by something troubles, connection have to stop.

Static IP Address

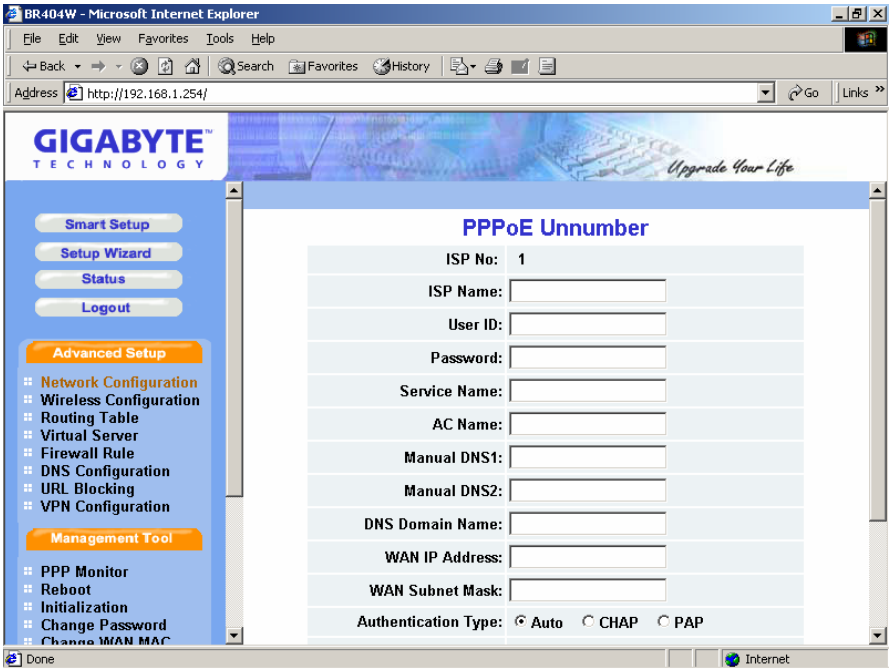


◈ ***ISP Name, WAN IP Address, WAN Subnet Mask, WAN Gateway, DNS1 and DNS2, DNS Domain Name***

Those information are provided by your ISP company. If your ISP company gives you more than one IP address, and then select one of them to fill in the above form.

PPPoE Unnumber

PPPoE unnumbered is a kind of PPPoE service provide by ISP. Using PPPoe unnumbered, customer could having more than 1 global IP address. Maybe 8 or 16, or more, it's all depend on ISP's server policy. One of these address should use for router's wan IP address, others could be use behind the router.

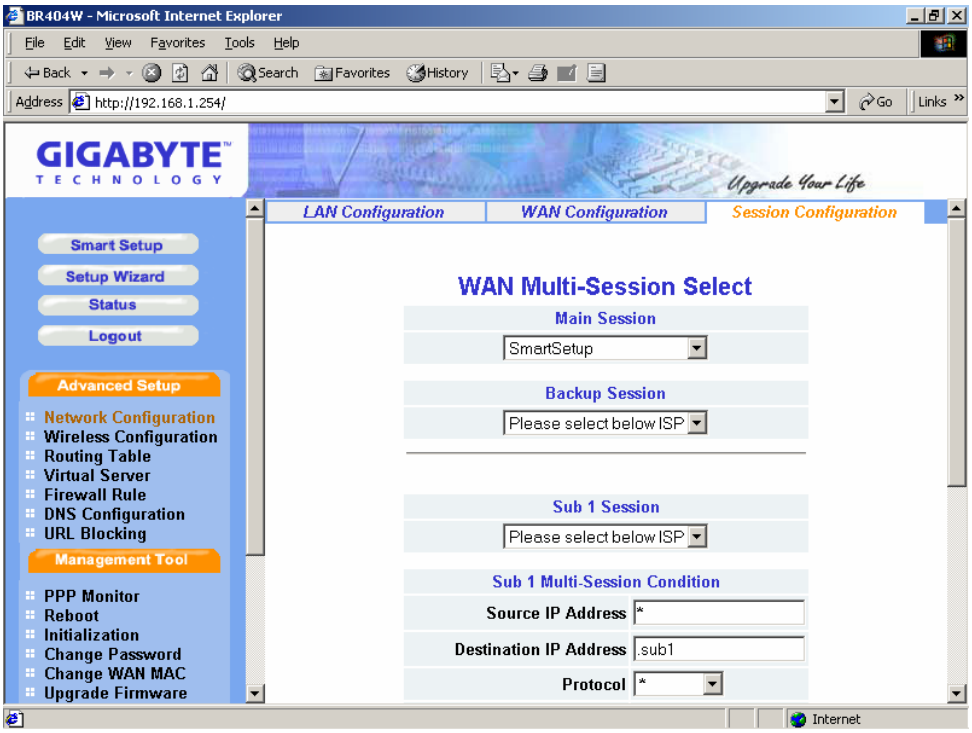


◈ ***ISP Name, User ID, Password, Service Name, AC Name, DNS1 and DNS2, DNS Domain Name, WAN IP Address, WAN Subnet Mask***

Those information are provided by your ISP company.

■ Multisession Configuration

The Multisession configuration allows you to setup the priority of WAN connection after you complete the WAN configuration. In our PPPoE multi-session, three connections will be established in three visual interfaces. Each interface owns ip address, gateway and netmask belong each sub network. So we can use a set of rule to routing packet. Which packets all information is matched of rules, it will be routing to different gateway.



On the PPPoE connection when established one connection peer to peer is call session. If we have multi PPPoE connect at the same time. We must have way to manager each session.

◈ *Backup Session*

User can set the alternate session to the main session as the backup session. In addition, if main session is fail to connection a backup session is replace main session.

For example,

The main session could not connect to an ISP.

Further the backup session could not connect too, the main session

Automatic : main -> backup->main->backup…….

Manual : main->backup (Backup tries to connect once only.)

Session keep alive was no response after the main session connected. Sub1 or

Sub2 session have no backup sessions. Backup session can be set the main session only.

Note: *The backup session can be specified LAN type connection.*

◈ ***Our priority of rule***

SUB2 > SUB1 >MAIN

In other words, every packets pass thought the router would be matching SUB2 rule first. If it is match, packet next hop will be change to SUB2 session gateway. If it is not, the Router check packet information matched with SUB1 rule. If it still not matched that will be route to main session gateway.

Note:

1. *Rule could be overlap for any condition.*
2. *All of rule in one session must be match.*
3. *Check order is SUB2->SUB1->MAIN, if any session rules matched. It will jump out the check order.*
4. *Main session is default session. All of packets match fail will be group under main session.*

Exception:

1. If sub session connection fail, the rule also to break down. Another session route path is alive. Packet will pass thought this session. It seems backup the sub session use main or sub1.
2. If main session is unlink or connection fail, sub1 and sub2 still by pass the match packet.
3. Each session are independent with NAT address translation.

◈ ***The method of setting IP address:***

IP Address	Description
*	All IP address
192.168.1.3	Specific IP address
192.168.1.0/24	Network address(24bit netmask)
192.168.1.3–192.168.1.33	Range assigned Separated by “–” ; no space
192.168.1.3,192.168.0.8	To allocate Separated by comma “,” ; no space

No assigned	Ignored

◈ ***The method of setting Host Name:*** (The destination IP can be assign to the IP address or Host name)

For example as follows:

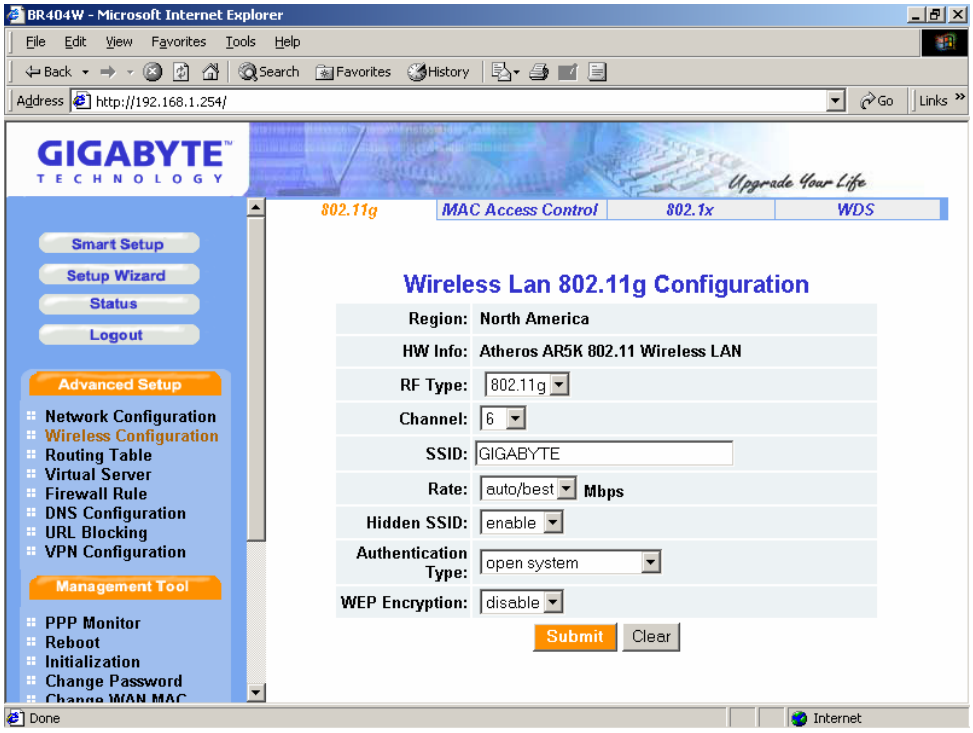
Host Name
.tw
.com.tw
www.gigabyte.com.tw
host1.www.gigabyte.com.tw
www.*.com.tw
No assigned

◈ ***The method of setting Port:***

IP Address	**Description**
*	All ports
80	Specific port
80–110	Range assigned Separated by “–” ; no space
80,8088	To allocate Separated by comma “,” ; no space
No assigned	Ignored

3-4-2. Wireless Configuration

■ Wireless LAN Configuration



◈ ***Region***

Because of the different region has a different open channel regulation, please check whether the default region value is your local area. If it did not appear properly region please contact your local distributor or authorized reseller immediately.

◈ ***HW info***

The information of the Wireless Lan Card.

◈ ***RF Type***

The option of the RF type is depend on your WLAN Card. If your WLAN Card supports the network standards of IEEE 802.11b and 802.11g, then the option will have two setting you can select.

◈ ***Channel***

Please choose the channel, which you can get best performance. Normally, it doesn't need to change. The default value is channel 6.

- ***SSID***

  The SSID is the name represent the router in the wireless network. This SSID string is case sinsitive of up to 32 ASCII characters. The default value is “GIGABYTE”, if the setup value is the default value, like “router”. Only can accept the computer connection, which use the wireless card SSID (or ESSID) set up, is “router”.

- ***Rate***

  You can select one of the rates among 1M, 2M, 5.5M and 11M based on your need. The default value is “**auto/best**”.

- ***Hidden SSID***

  This setting allows you to hide the SSID in wireless transmission. Those who don’t know the SSID will be able connect to the router. The default value is “**disable**”.

- ***Authentication Type***

  You may choose between “**Open System**”, “**Shared Key**”, “**WPA Radius with 802.1x**” and “**WPA Pre-shared key**”. The Authentication Type default is set to “**Open System**”.

  Open System, in which the sender and the recipient do NOT share a secret key. Each party generates its own key-pair and asks the receiver to accept the randomly generated key. Once accepted, this key is used for a short time only. Then a new key is generated and agreed upon.

  Shared Key is both the sender and the recipient share a secret key.

  If the “**Shared Key**” option is selected, and then the option “**disable**” of the WEP will be disabled.

  WPA adius with 802.1x, if you have been using Wi-Fi for a while, you are probably familiar with the 802.1X authentication protocol. This protocol allows users to authenticate into a wireless network by means of a RADIUS Server. In standard Wi-Fi, 802.1X authentication is optional. However, 802.1X authentication is a requirement for WPA. If your environment does not have a RADIUS server in place, you can still use WPA in spite of the 802.1X requirement. As an alternative to RADIUS, WPA supports the use of a preshared key.

WPA Pre-shared key, One of the biggest drawbacks to traditional WEP security is that changing the encryption key is optional. Even if you do switch encryption keys from time to time, there is no option for globally rekeying all access points and all wireless NICs.
Instead, rekeying is a tedious manual process and is completely impractical for large organizations. After all, the instant you rekey an access point, none of the clients will be able to access it until they are also rekeyed.
But with WPA, the rekeying of global encryption keys is required. In the case of unicast traffic, the encryption key is changed after every frame using Temporary Key Integrity Protocol (TKIP). This protocol allows key changes to occur on a frame by frame basis and to be automatically synchronized between the access point and the wireless client. Global rekeying works by advertising the new keys to wireless clients.
The TKIP is really the heart and soul of WPA security. TKIP replaces WEP encryption. And although WEP is optional in standard Wi-Fi, TKIP is required in WPA. The TKIP encryption algorithm is stronger than the one used by WEP but works by using the same hardware-based calculation mechanisms WEP uses.
The TKIP protocol actually has several functions. First, it determines which encryption keys will be used and then verifies the client's security configuration. Second, it is responsible for changing the unicast encryption key for each frame. Finally, TKIP sets a unique starting key for each authenticated client that is using a preshared key.

◈ **WEP Key**

Protects your information with the highest level of industry-standard WEP encryption: 64/128/152-bit for 802.11b standard, and up to 152-bit for 802.11g standards. When the “Disable” is selected there is no WEP encryption. When “64bits”, “128bits” or “152bits” selected there is encrypted date transfer to prevent unauthorized user to access the wireless network.

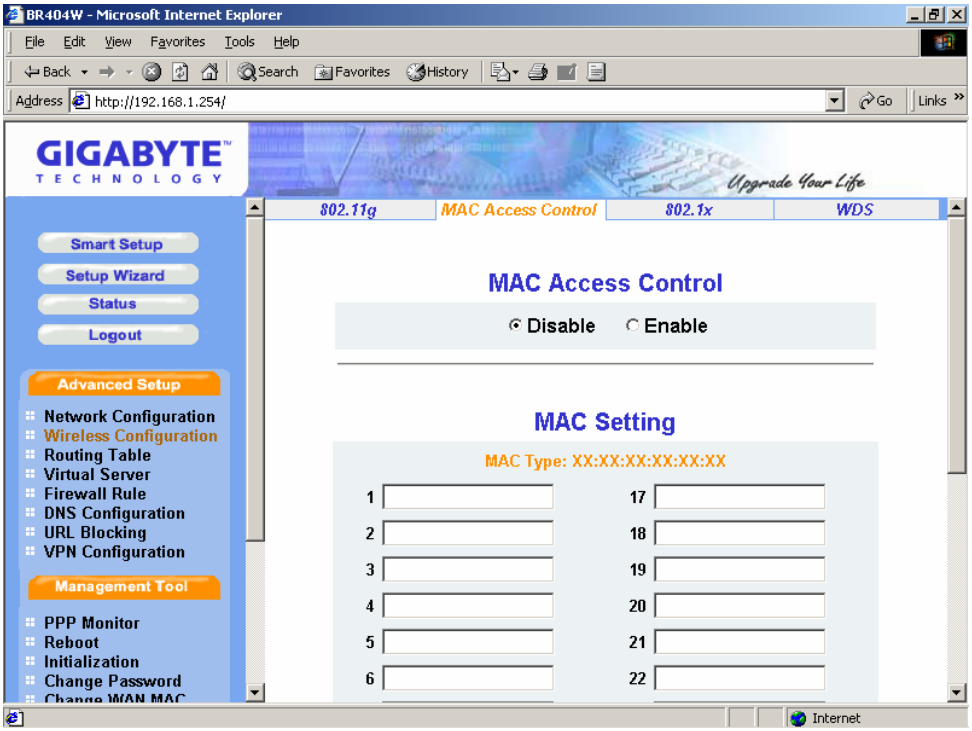
There are three levels of encryption 64 bits, 128 bits and 152bits. The 64 bits encryption is referenced as a lower level encryption. The 152 bits encryption is referenced as a higher level encryption.

The 64 bits WEP encryption use 40 bits as a secret key, which can controlled by user, and 24 bits as the initialize vector, which user can not control. These two portions plus together is 64 bits encryption. Some other vendor’s product might refer as 40 bits encryption. It is the same thing.

The 128 bits WEP encryption use 104 bits as a secret key, which can controlled by user, and 24 bits as the initialize vector, which user can not control. These two portions plus together is 128 bits encryption. Some other vendor's product might refer as 104 bits encryption. It is the same thing.

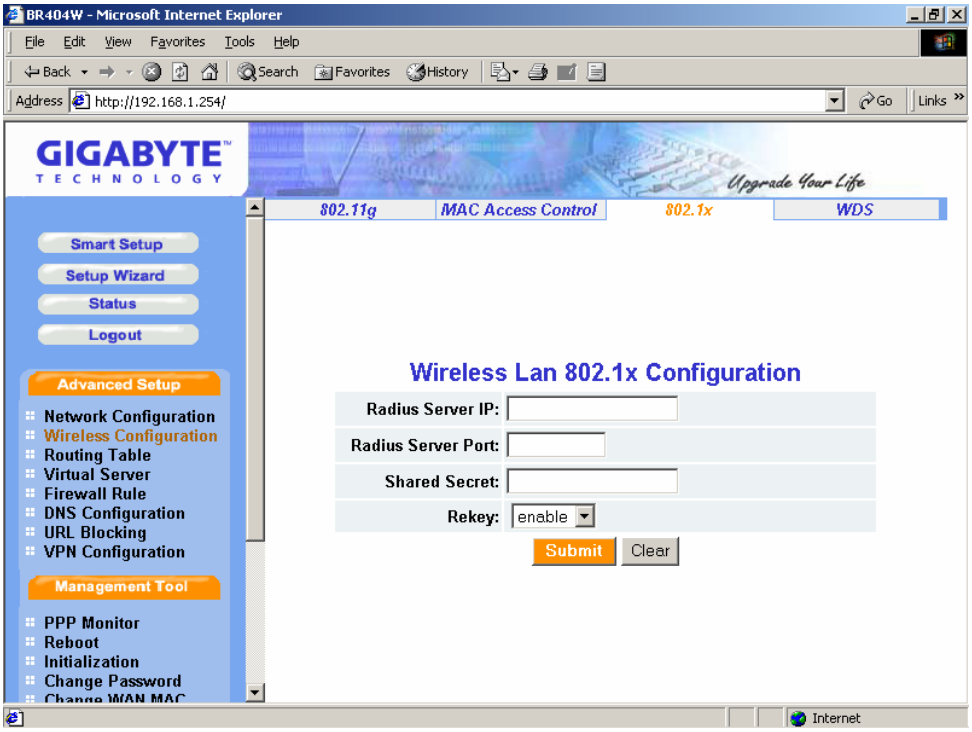
The 152 bits WEP encryption use 128 bits as a secret key, which can controlled by user, and 24 bits as the initialize vector, which user can not control. The 152 bits WEP encryption spawns a KEY ID containing 32 HEX digits.

■ MAC Access Control of the Wireless

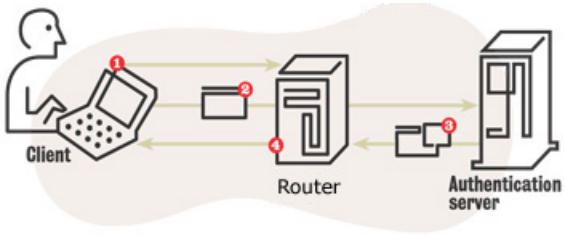


The MAC Access Control allows the router to define up to 32 hosts which are allowed to access to the WAN port. To disable the MAC Access Control function, keep the default value, **Disable**. To set up a MAC setting, click **Enable**.

■ 802.1x



802.1x authentication for wireless LANs provides centralized, server-based athentication of end users.



1) A client sends a “start” message to a router, which requests the identity of the client.
2) The client replies with a response packet containing an identity, and the router forwards the packet to an authentication server.
3) The authentication server sends an “accept” packet to the router.
4) The router places the client port in authorized state, and traffic is allowed to proceed.

◈ ***RADIUS server IP***

Please assign a IP address to the RADIUS server IP(authentication server).

◈ ***RADIUS server Port***

The setting range is 1~65536.

- ***Shared sercet***
  This filed can key in up to 256 character.

- ***Rekey***
  Under this option two setting are possible: “**enable**” or “**disable**”. The default value is “**enable**”.

■ WDS

Wiring is headache and complex problem on the Networking environment all the time. The Wireless Access Point solves the connection problem between end-users and the backbone of the network. But it still is requiring establishing a wired backbone network on this framework.

Wireless Distribution System (WDS), the technology provide a method that use “Wireless” to take place of the wired backbone networking, allows several of the access points to compose a wide Wireless LAN network. However, even if the general business or home use, the access point with WDS function has decreased the difficultly of the wired wiring. On the real network environment, it is still need to use wired method to connect router and access point when they want to link ISP to Internet.

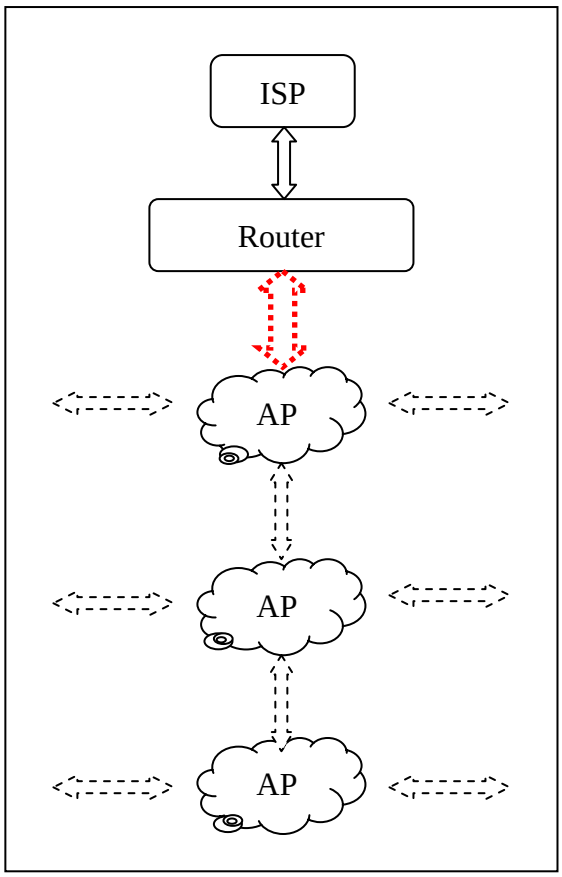
In order to built an entire wireless solution to get rid of the wiring problem. Integrate the technology of the WDS and Routers that connect the routers and access points through the WDS has created the concept of the Wireless Distribution.

Advantage:

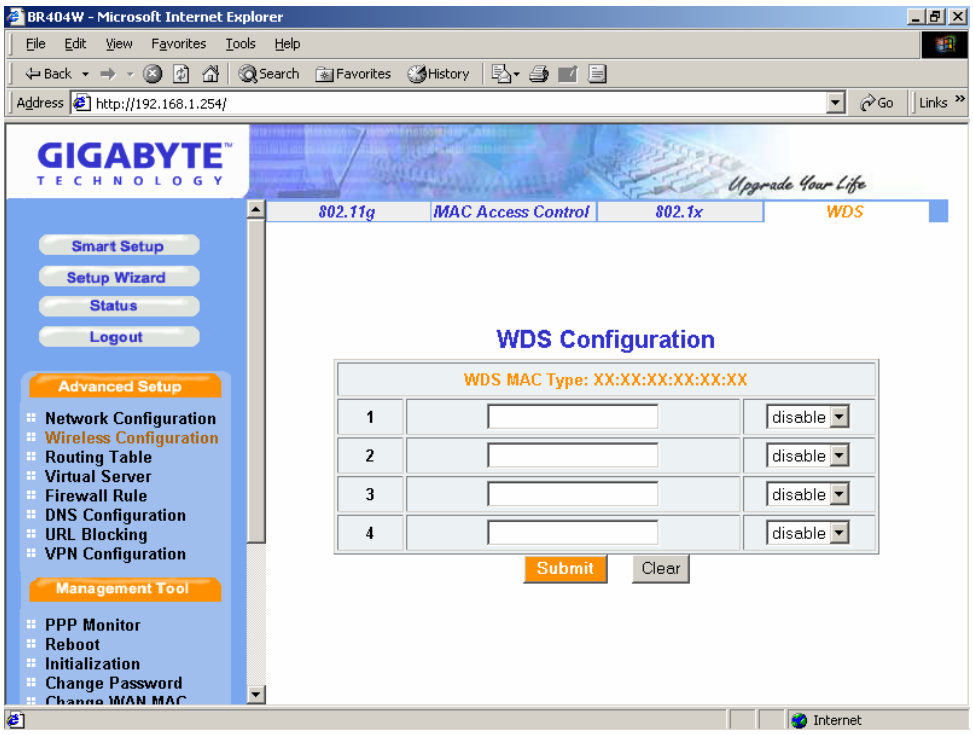
1. **Convenience Environment**: It gets rid of the wiring problem and allows all devices to connect through the Wireless LAN except the connection between the ISP and routers on the networking environment.

2. **Strong expansibility**: It can expand the network just add new access point directly where needs to have the network.

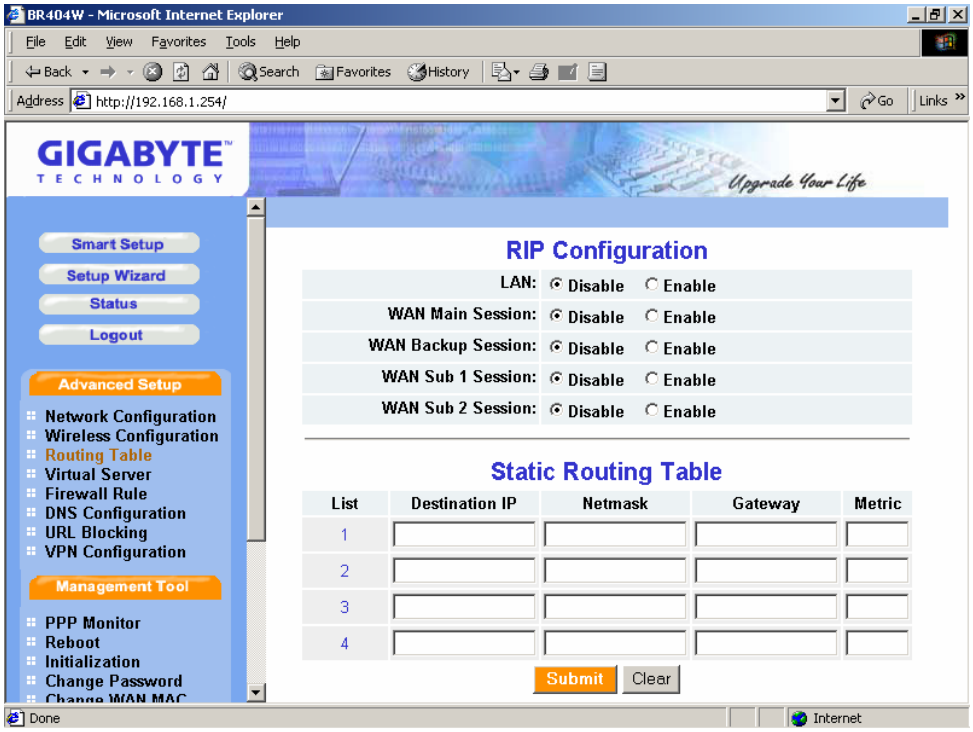
Extended Distributed
Wireless Systems（EDWS）



WDS could be used for extend wireless ambit for router. For example, router locate at floor 1, but the radio's range can't reach floor 3. In this case, customer can deploy a access point at floor 2 and then enable WDS function of router. Then, user at floor 3 can connect to rooter at floor 1 though access point at floor 2.



3-4-3. Routing Table



■ **RIP Configuration**

RIP(Routing Information Protocol) is a dynamic internetwork routing protocol primary used in *interior* routing environments. A dynamic routing protocol, as opposed to a static routing protocol, automatically discovers routes and builds routing tables.

■ **Static Routing Table**

Under some of Internet environments, some of the subnet do not go through the default gateway. Users can add those routing information to Static Routing Table themselves.

◈ ***Destination IP***

The Destination IP address is the address of the network or host to which the static route is assigned.

◈ ***Netmask***

The Netmask determines which portion of a destination LAN IP address is the network portion, and which portion is the host portion.

- ***Gateway***
  This is the IP address of the gateway device that allows for contact between the router and the network or host.

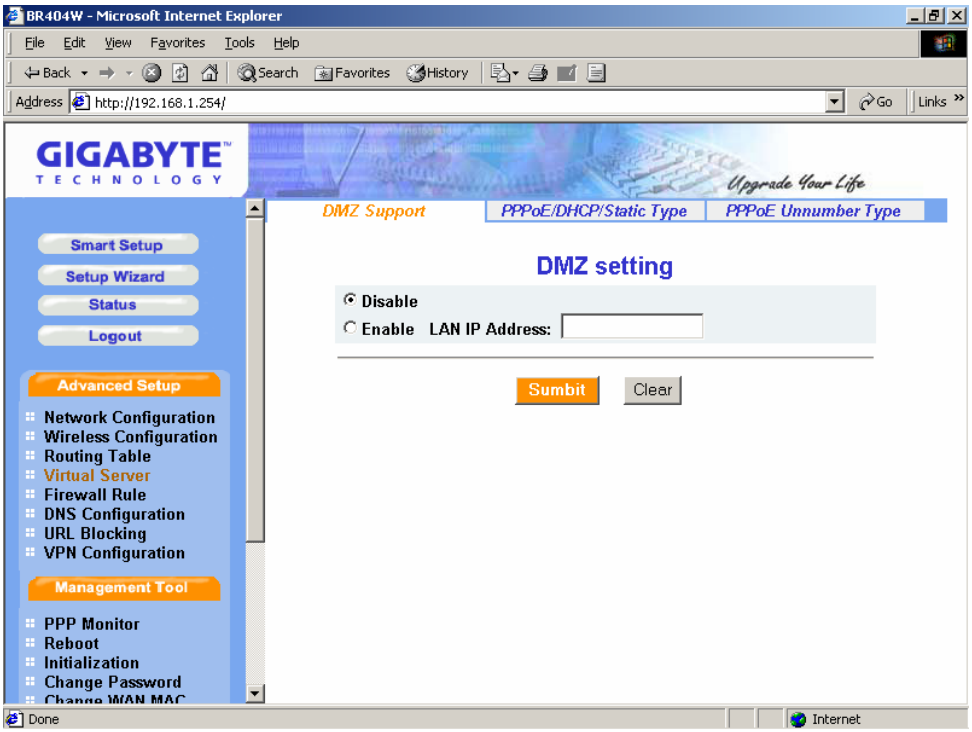
- ***Metric***
  Type a numeber between 1 and 15 as the Metric value. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set is to 1. The default value is 1.

Verify the desired setting and then click the "**Submit**" button to set the value into GN-BR404W.

3-4-4. Virtual Server

Virtual server setting split into two different case. Case 1 is router having only 1 global IP address, PPPoE/DHCP/Static is this case. Case 2 is router having more than 1 global IP address, normal having 8 or 16 IP address, PPPoE unnumbered is this case. In case 1, virtual server only need to configure LAN host information, because WAN IP address always the same, but in case 2, virtual server also need to configure which WAN IP address need redirect to internal LAN host.

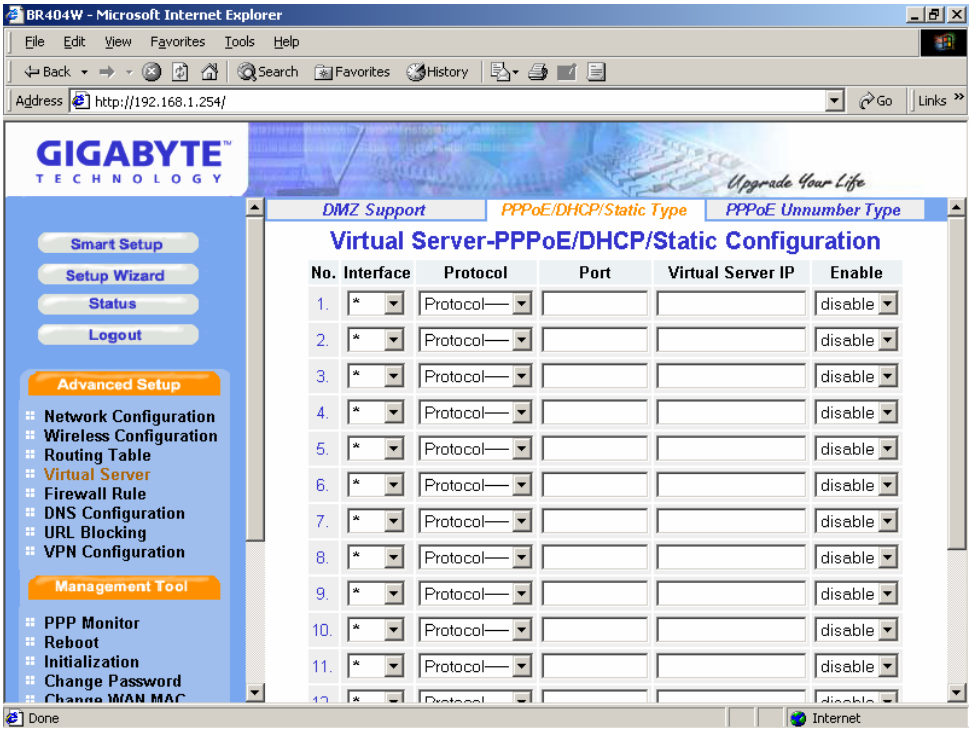
- **DMZ Support of the Virtual Server**



If you have a computer that cannot run an Internet application (e.g. internet game, vedio conferencing, or VPN connections) properly from behind the NAT firewall, or set up a server which can connect to the Internet in the Intranet then you can open the computer up to unrestricted two-way Internet access.To use the DMZ, you have to set a static IP address for the computer. The IP Address (such as 192.168.1.2) of the computer at the LAN terminal can be used to input to the field of LAN IP Address.

Verify the desired setting and then click the "**Submit**" button to set the value into GN-BR404W.

■ PPPoE/DHCP/Static Type of the Virtual Server



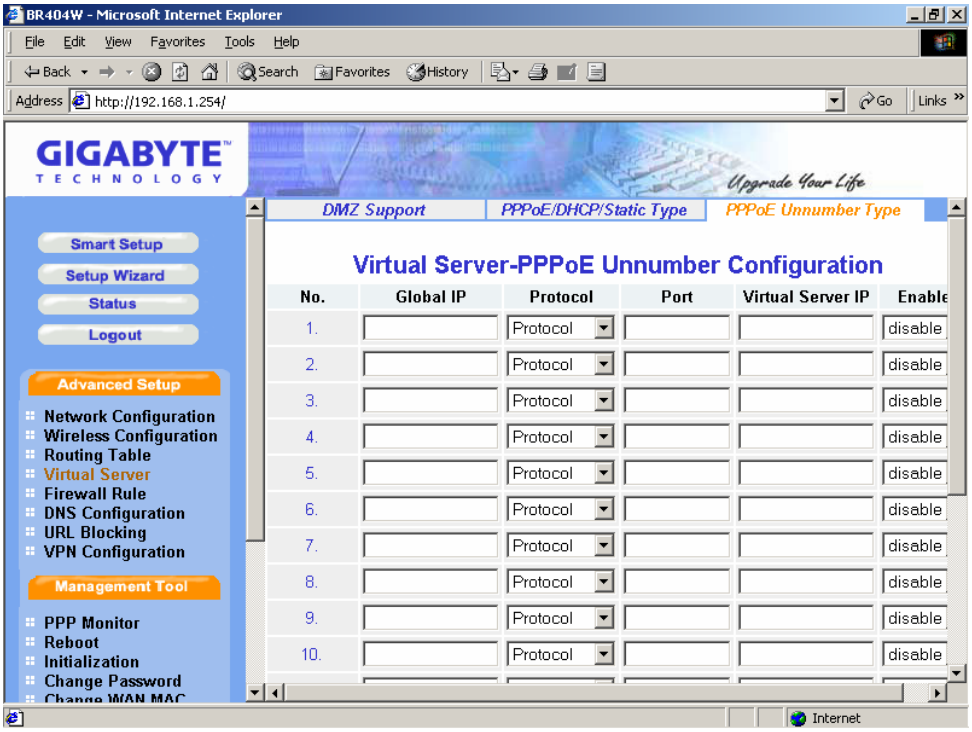
Virtual Server provides a way to let the PC at the WAN end connect to a server of a PC at the LAN end. Taking the IP address 192.168.1.1 of a PC on a FTP at the LAN for example:

➔ Protocol: TCP
➔ Port: 21
➔ Vitrual Server IP: 192.168.1.1
➔ Enable: enable

The PC at the WAN end can connect to the internal FTP server at the IP address 192.168.1.1 via the WAN end of the IP address of the FTP BR404W.

Interface : ***** means "**all**",
1 means "**Main session**",
2 means "**Sub1 session**",
3 means "**Sub2 session**"

■ PPPoE Unnumber Type of the Virtual Server



The PPPoE Unnumer user may have multiple global IP addresses, therefore each IP address needs to setup specifically.

Your ISP may provides you a group of the Global IP,
e.g. 61.222.10.1 ~ 61.222.10.7(But only can use 61.222.10.2~61.222.10.6)

Taking the IP address 192.168.1.1 of a PC on a FTP at the LAN for example:

- Global IP: 61.222.10.2
- Protocol: TCP
- Port: 21
- Vitrual Server IP: 192.168.1.1
- Enable: enable

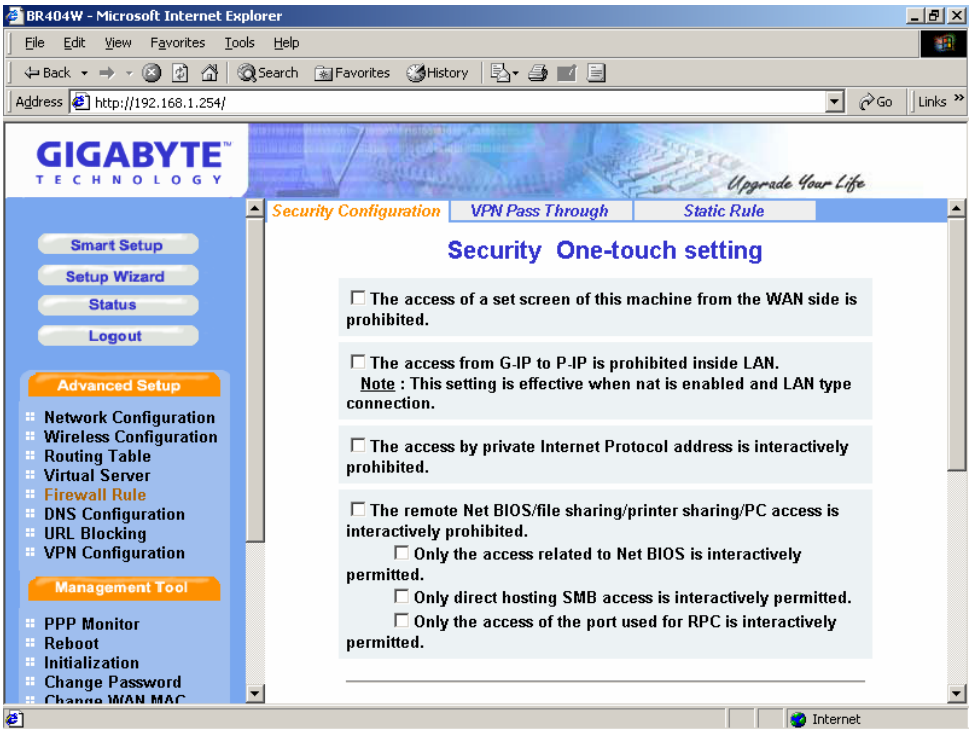
The PC at the Global IP 61.222.10.2 can connect to the internal FTP server at the IP address 192.168.1.1 via the WAN end of the IP address of the FTP BR404W.

3-4-5. Firewall Rule

The Firewall Rule allows you to configure your own security policy to prevent unauthorized Internet users from accessing private networks or corporate LAN's and Intranets.

■ Security Configuration

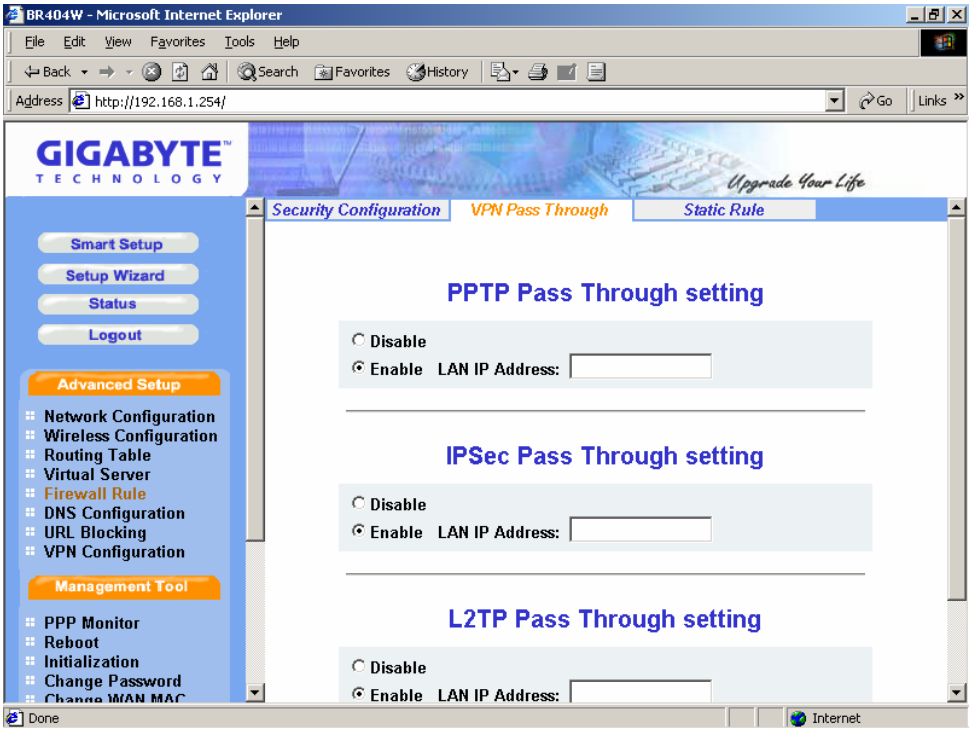
The security configuration provides a security list for you configure, includes Security One-Touch Setting, Stealth Mode, and Unlawful Computer Access Detection.



From this security setting list, you can check which you want and then click "**Submit**" button to set the value into GN-BR404W.

Note: *"URL Blocking" function will not work when any of the item from "Security one-touch setting" as well as the" The full state packet inspection is used" under "Unlawful computer access detection" function is clicked.*

■ VPN Pass Through



Virtual private networks (VPN)are secured private network connections, built on top of publicly-accessible infrastructure, such as the Internet or the public telephone network. VPNs typically employ some combination of encryption, digital certificates, strong user authentication and access control to provide security to the traffic they carry. They usually provide connectivity to many machines behind a gateway or firewall.

GN-BR404W supports Internet-industry standards technology to provide customers with open interoperable VPN solutions such as Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP) as well as Point-to-Point Tunneling Protocol (PPTP).

◈ ***PPTP Pass Through setting***

PPTP stands for Point-to-Point Tunneling Protocol. It basically allows you to establish a connection to a corporate network and you can share files and other data as if your machine were actually on that local network.

◈ ***IPSec Pass Through setting***

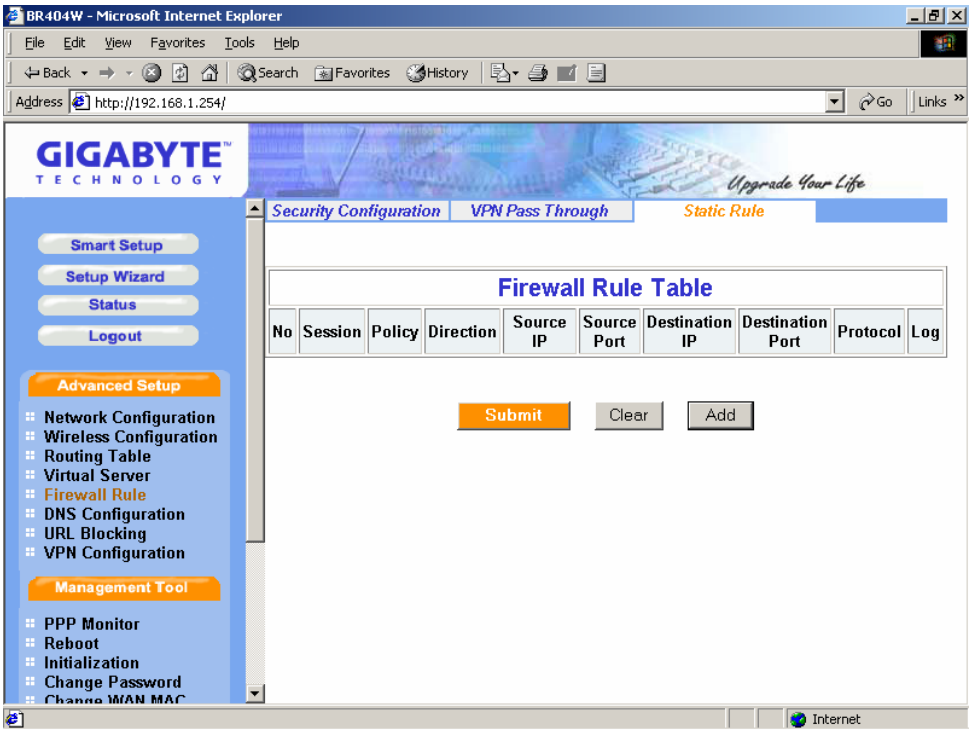
IPSec stands for IP Security. It provides authentication and encryption over the Internet. It functions at Layer 3 and thus secures everything on the network. It has become a standard protocol used for virtual private networks (VPNs).

◈ ***L2TP Pass Through setting***

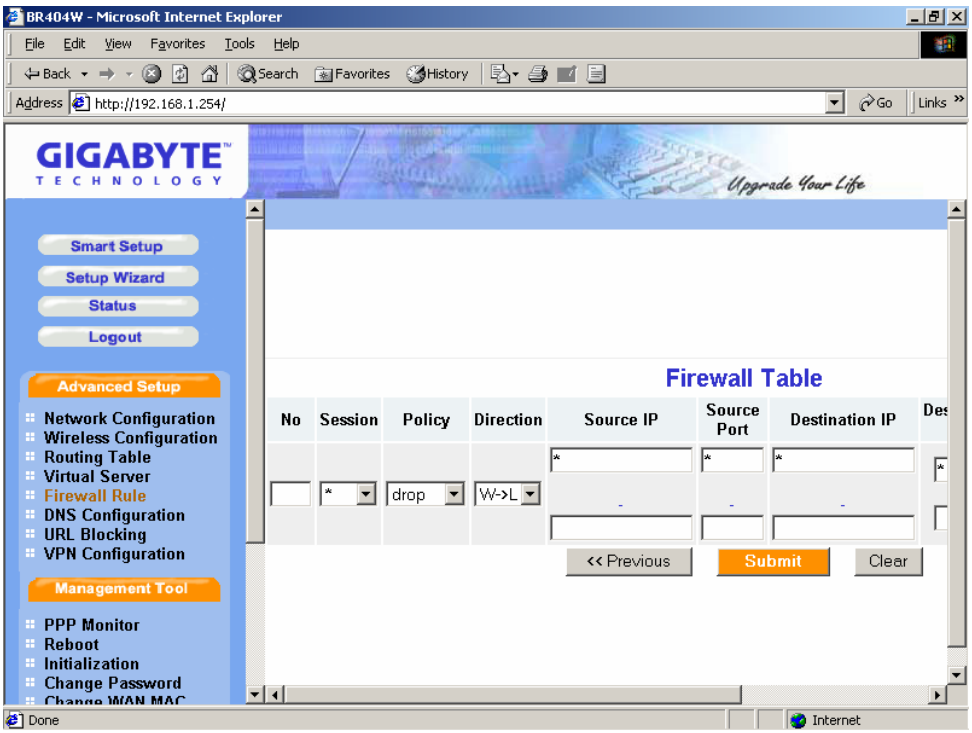
L2TP stands for Layer 2 Tunneling Protocol. It is an extension of the Point-to-Point Tunneling Protocol and is also used to establish virtual private networks.

Enable/Disable VPN pass through. If administrator configure a host to enable VPN pass through, router will automatically setting virtual server and firewall setting for this host. All VPN packets will be transparent and will redirect to this host. VPN pass through works, either VPN server behind the LAN side or VPN server locate at WAN side. For different VPN pass through setting, only 1 host can be configured as pass through.

■ Static Rule



This screen allows you to edit the firewall rule table manually. It helps protect your local network against attack from outside and provides a method of restricting users on the local network from accessing the Internet. Additionally, it can filter out specific packets to trigger the router to place an outgoing connection. Please click "**Add**" to edit the rule table, there will appear the screen as shown below.



◈ ***Rule Number (No.)***

From 1~64, rule 1 has highest priority, rule 64 has lowest priority

◈ ***Policy***

Under this option two settings are possible: "**accept**" or "**drop**".

◈ ***Direction***

Sets the direction of packet flow. For the Data Filter:

a. **W->L**, WAN to LAN, specifies the rule for filtering incoming packets.

b. **L->W**, LAN to WAN, specifies the rule for filtering outgoing packets.

◈ ***Protocol***

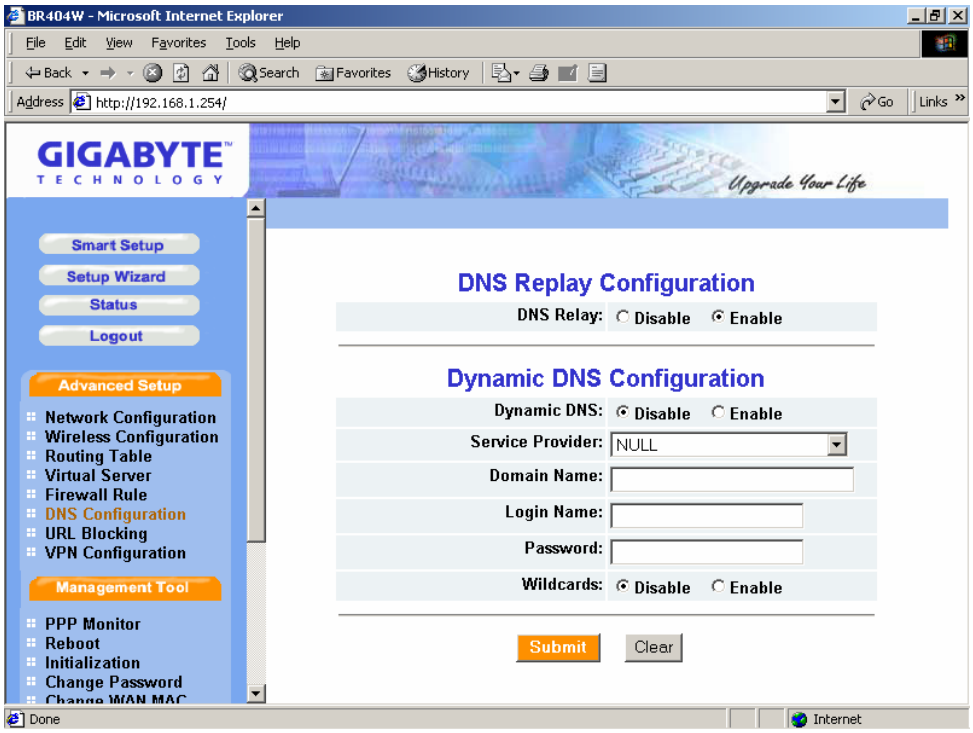
Specifies the protocol(s) this static rule will apply to. Under this option eight settings are possible: "**TCP**", "**UDP**", "**TCP & UDP**", "**TCPEST**", "**ICMP**", "**GRE**", "**ESP**", "*****".

◈ ***Log***

Enable or disable the log function for this rule.

Verify the desired setting and then click the "**Submit**" button to set the value into GN-BR404W.

3-4-6. DNS Configuration



- **DNS Replay**

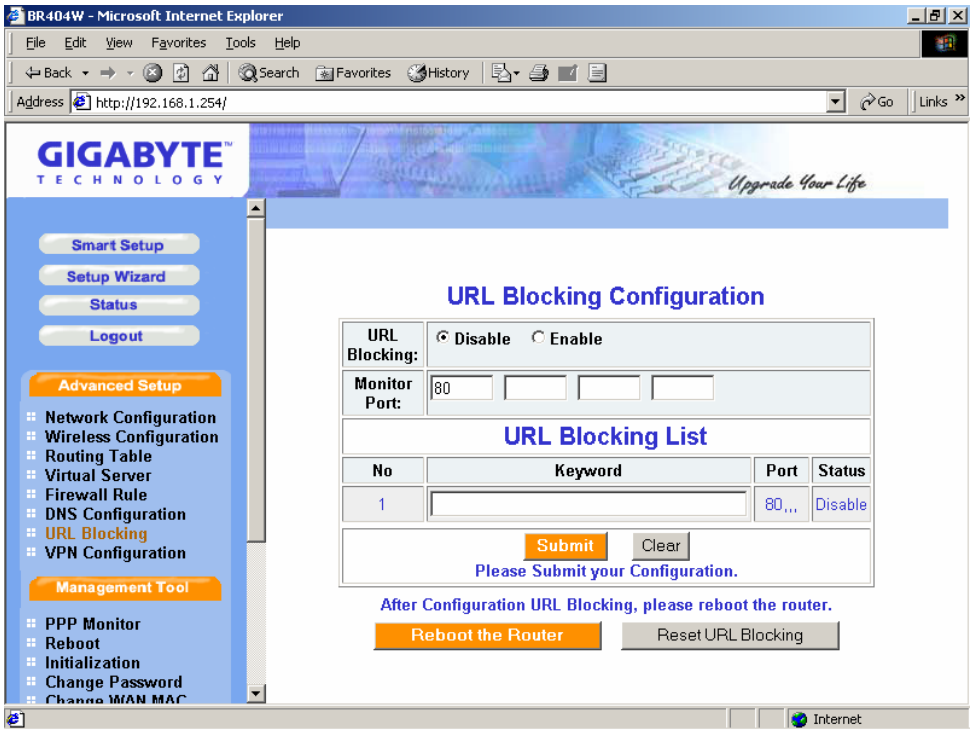
  The default value of the DNS replay is "**Enable**". The DNS query packets will send through the router. When a DNS query packet enters the router, and the router will sends an answer to the host that sent the DNS query packet. And then users have to set the IP address of the router as the IP address of the DNS.

- **Dynamic DNS**

  The Router offers a Dynamic Domain Name Server service. The Dynamic DNS allows you to assign a fixed host and domain name to a dynamic Internet IP address. It is very useful when combined with the "Virtual Servers" feature. It allows Internet users to contact to your virtual severs using a URL, rather than an IP address. Before you to use this feature, please register for an account with one of the dynamic DNS service at http://www.dyndns.org.

  1. You can **Disable** or **Enable** the Dynamic DNS service.
  2. Select the name of your dynamic DNS service provider.
  3. Type the Domain Name(or Host Name) that your dynamic DNS provider gave you.
  4. Type the login Name(or Username) and Password for your dynamic DNS account.
  5. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Enable wildcard to active this function.

3-4-7 URL Blocking Configuration



The Router allows you to restrict access based on web address and web address keywords.

1. To disable the URL Blocking function, keep the default value, **Disable**. To set up a URL Blocking setting, click **Enable**.
2. To type a keyword or domain in the Keyword box.

Verify the desired setting and then click the "**Submit**" button to set the value into GN-BR404W. Or you can click "**Reset URL Blocking**" to reset the URL Blocking configuration.

After you configure the URL Blocking, please reboot the Router.

Note: *"URL Blocking" function will not work when any of the item from "Security one-touch setting" as well as the " The full state packet inspection is used" under "Unlawful computer access detection" function is clicked.*

3-4-8 VPN Configuration

A VPN is a secure, private communication tunnel between two or more devices across a public network (like the Internet). These VPN devices can be either a computer running VPN software or a special device like a VPN enabled router. It allows your home computer to be connected to your office network or can allow two home computers in different locations to connect to each over the Internet.

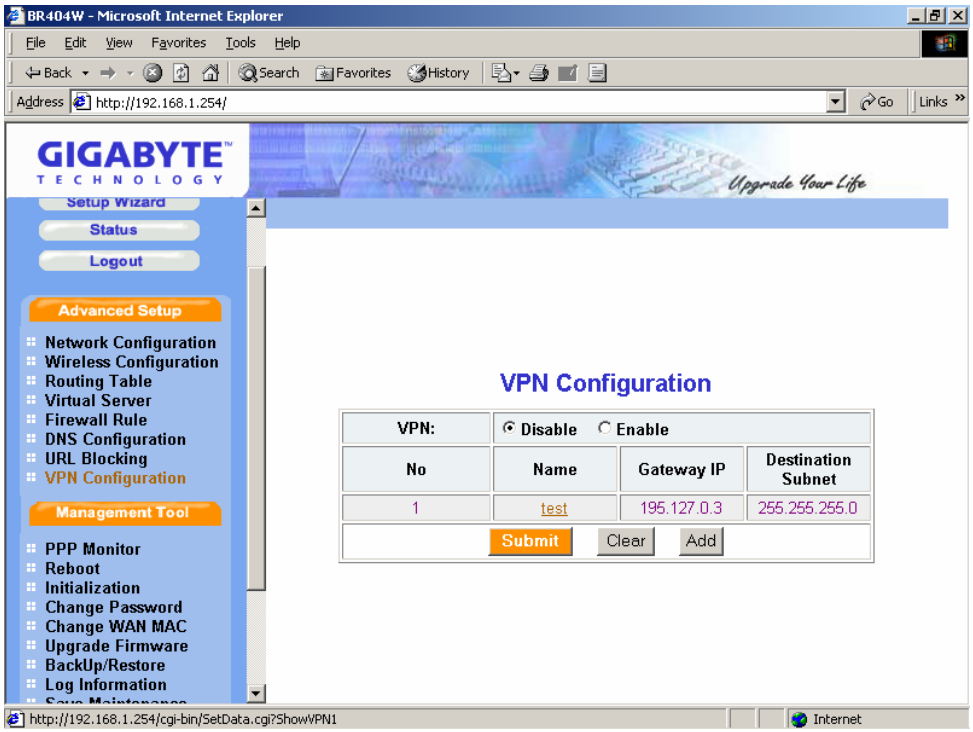
Clients and Servers

A VPN server is a piece of hardware or software that can acts as a gateway into a whole network or a single computer. It is generally ‘always on’ and listening for VPN clients to connect to it.

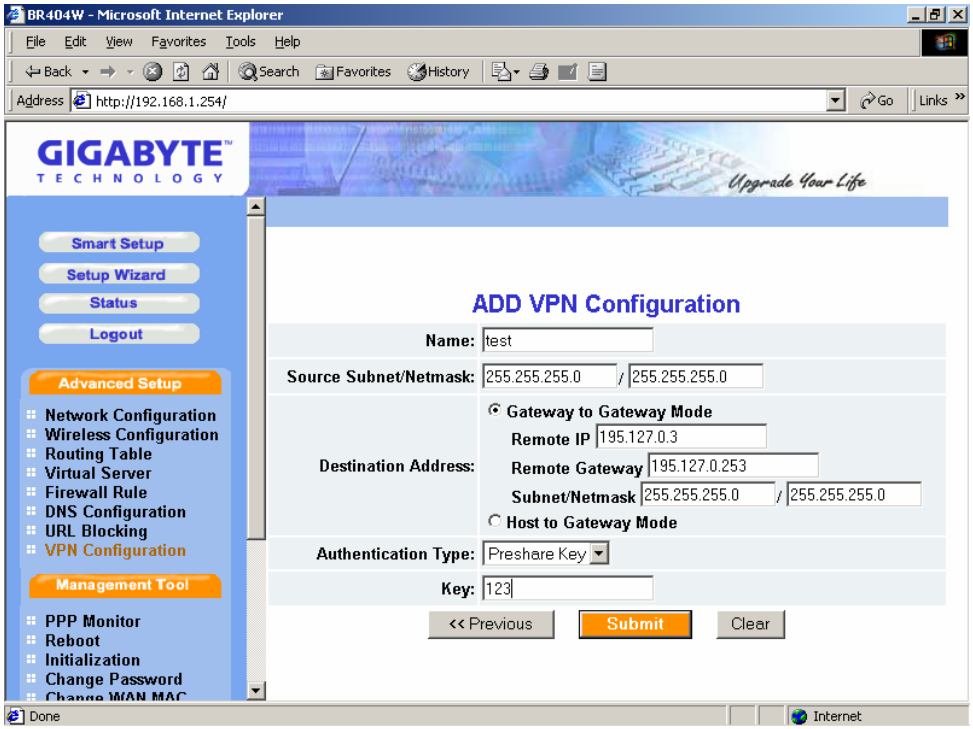
A VPN Client is most often a piece of software but can be hardware too. A client initiates a ‘call’ to the server and logs on. Then the client computer can server network can communicate. They are on the same ‘virtual’ network. Many broadband routers can 'pass' one or more VPN sessions from your LAN to the Internet. Each router handles this differently.

The Gigabyte router is a IPSec VPN which support following function:

1. Groups for Diffie-Hellman key negotiation - group 2, modp 1024-bit
2. Encryption transforms - Triple DES
3. Authentication transforms -HMAC using MD5



Click “Add” button to add a new VPN.



Name You can give a name for the VPN.

Source Subnet/Netmask Enter the router’s subnet.

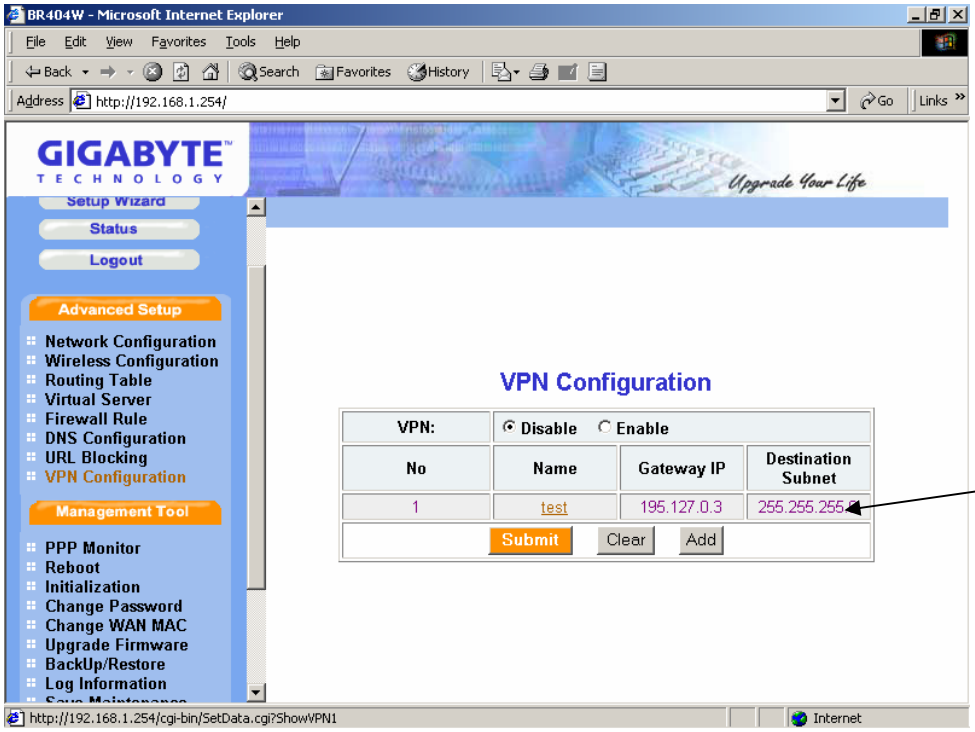
Destination Address

- Gateway to Gateway Mode, allows you to setup the connection of the router to another router. Please enter the remote(router2) IP address, Gateway address and subnet netmask.
- Host to Gateway, allows the PCs connect to the router.

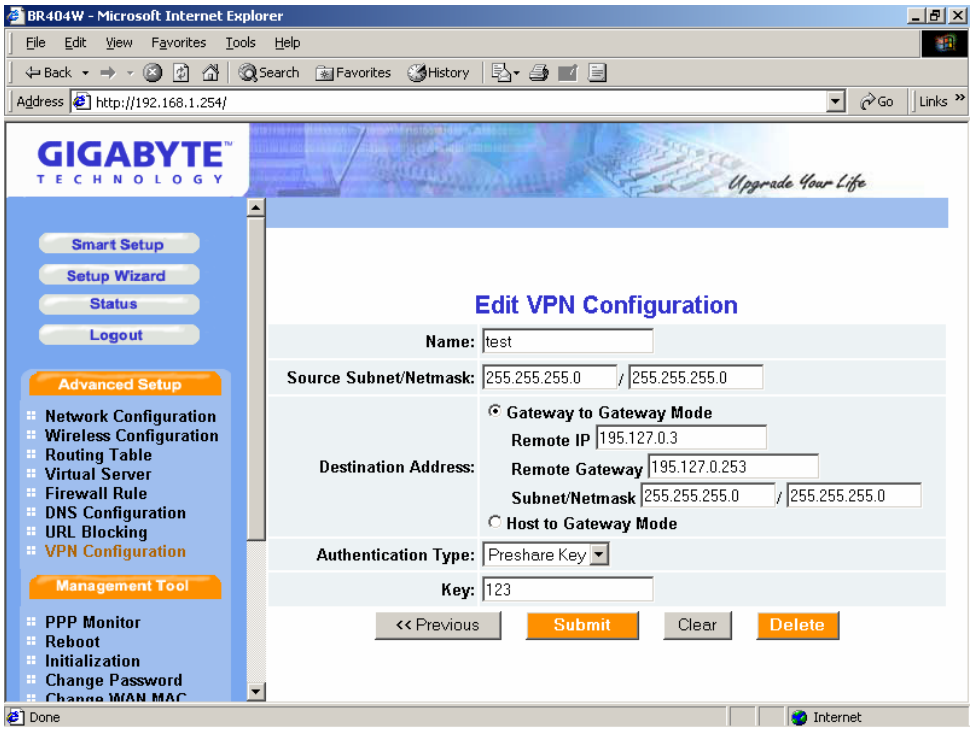
Authentication Type (Preshare Key) Please enter a key for the router to authorize each other.

Verify the desired setting and then click the “**Submit**” button to set the value into GN-BR404W.

Click the VPN hyperlink to edit the VPN configuration.



Click to edit the VPN configuration.

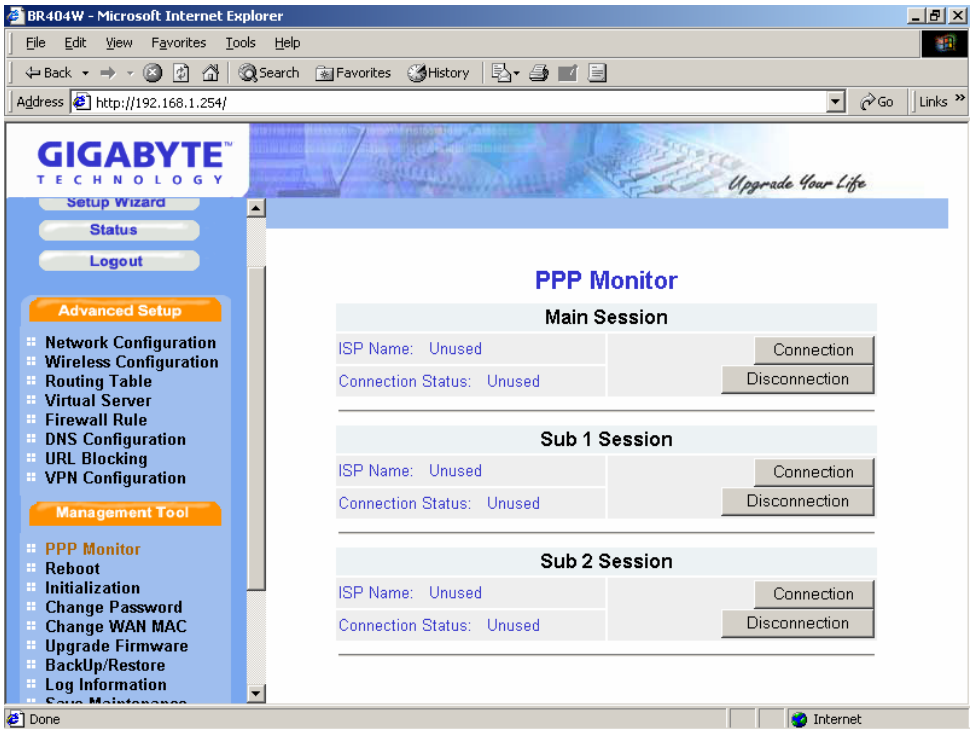


3-5. Management Tool

This section will show you how to use the management tool to manage and maintain your wireless broadband router.

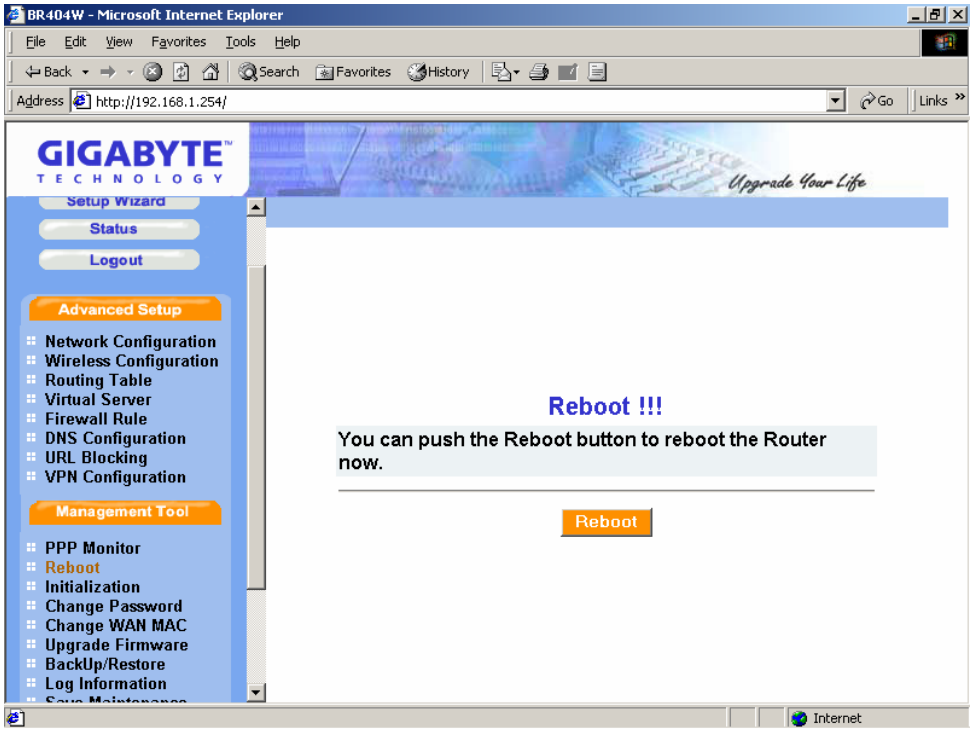
3-5-1. PPP Monitor

The PPP Monitor will show you the WAN connection status. We can disconnect ppp anytime by pressing the “disconnection” button. We also can connect to an ISP again by pressing the “connection” button. When each session connects to an ISP again, each session, which are main, sub1or sub2, inherits the attribute of previous connection.



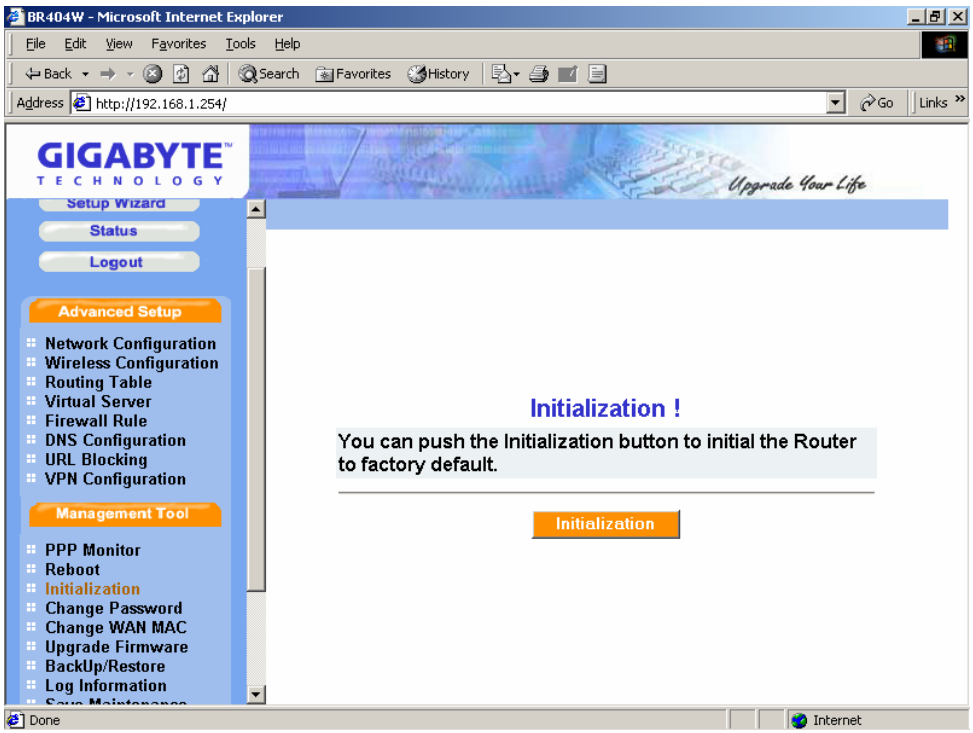
3-5-2. Reboot

This function allows you to restart the GN-BR404W.



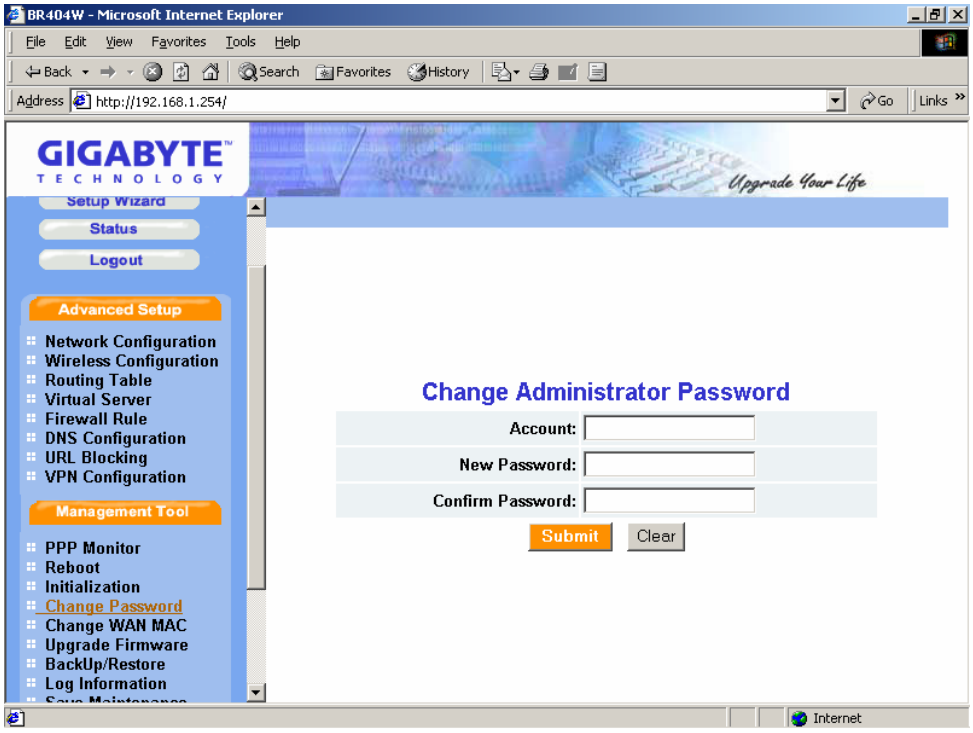
3-5-3. Initilization

You can use this function to initial the router to factory defult value. Or you can press the "**init**" botton on the GN-BR404W about 5sec, then the router will be restart and the system setting will restore to the factory default value.



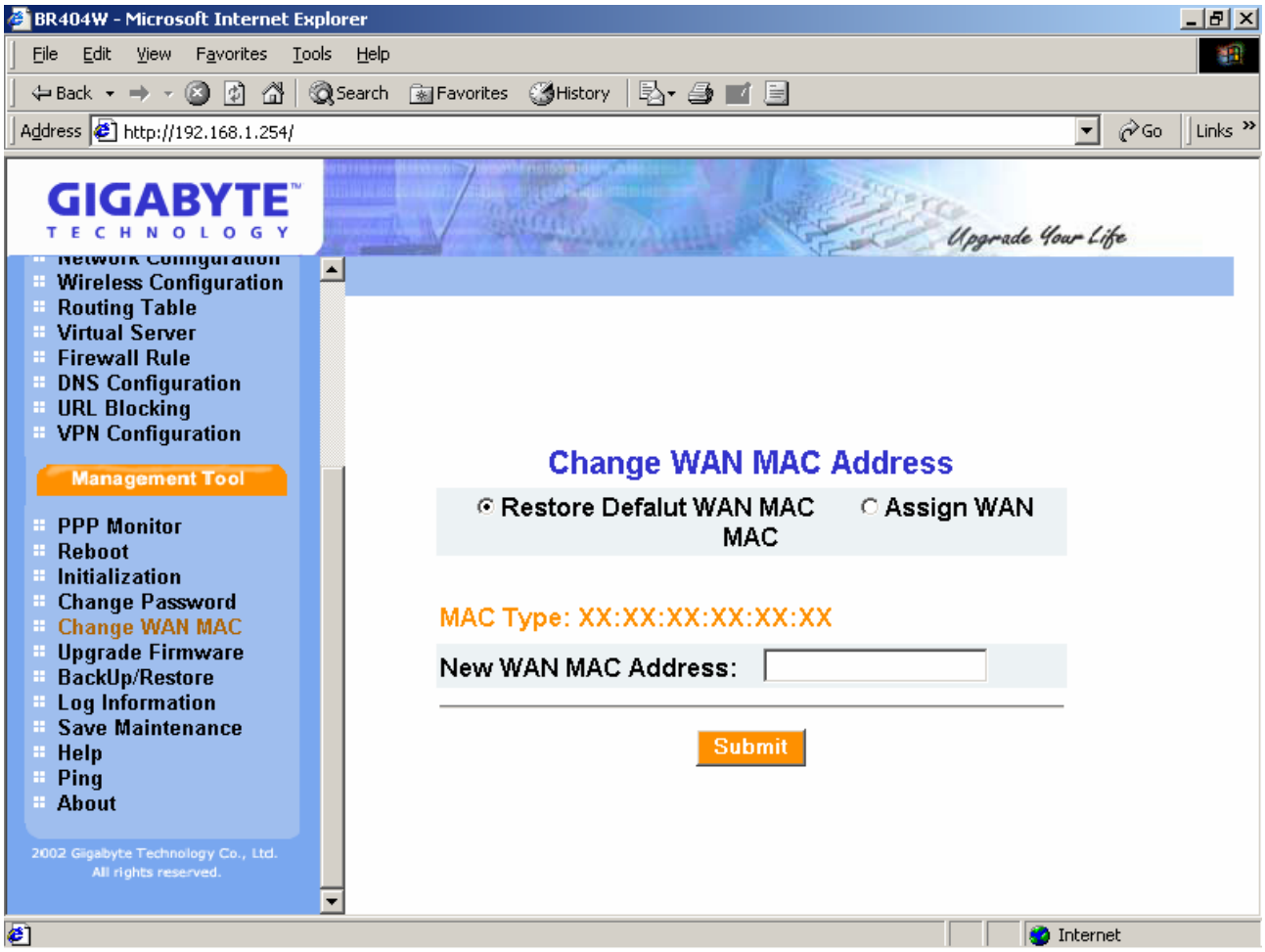
3-5-4. Change Password

User can change the administration password of the GN-BR404W to prevent other user access to the GN-BR404W. Please enter the account and a new password and confirm the password and then click "**Submit**". You have to enter this new password to log in when you want to configure the GN-BR404W next time.



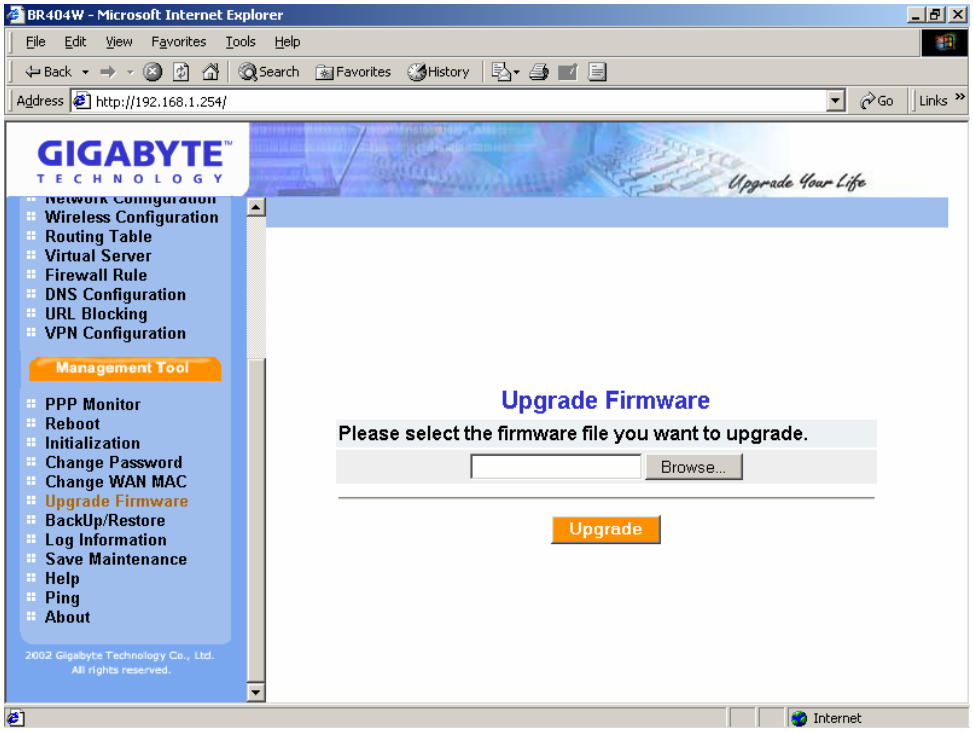
3-5-5. Change WAN MAC

If your ISP company asks you to use the original MAC address. You can select the "**Assign WAN MAC**" and enter the "**New WAN MAC Address**". The MAC address is from your Network Interface Card (NIC) that you registered with your ISP company. If you want to restore to the factory default value, please select "**Restore Default WAN MAC**". Verify the desired setting and then click the "**Submit**" button.



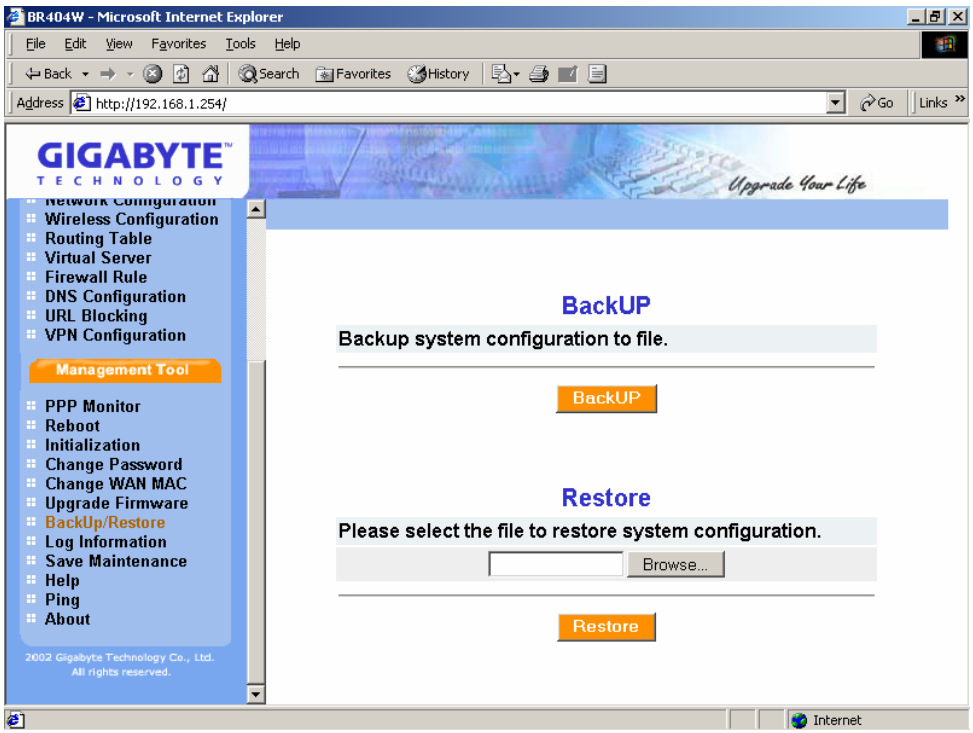
3-5-6. Upgrade Firmware

This tool allows you to upgrade the latest firmware of the GN-BR404W using a file provided by Gigabyte. You can download the upgraded firmware version from Gigabyte website. Please click "**Browse**" and select your desired upgrade file (firmware version), and then click "**Upgrade**".



3-5-7. BackUp Restore

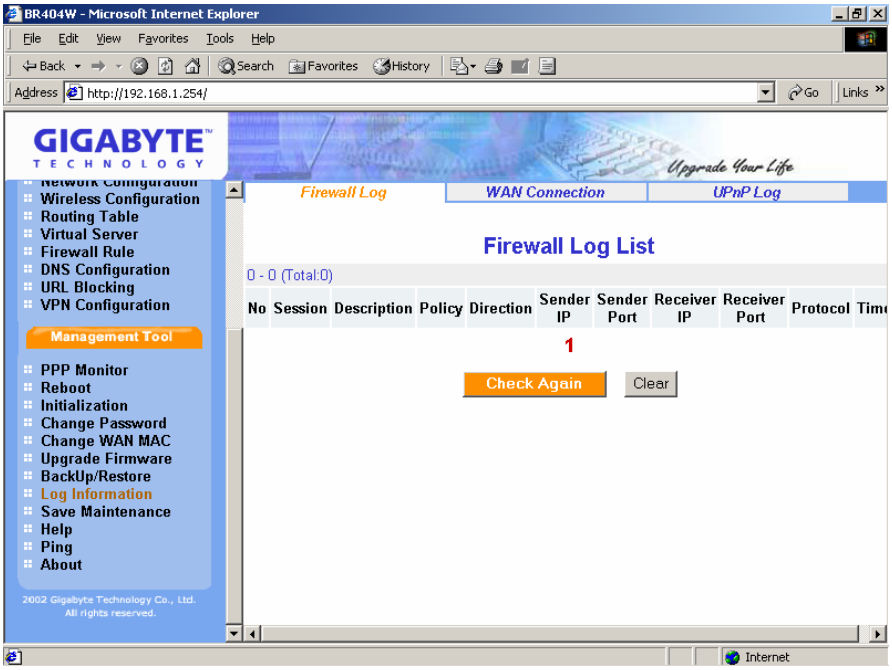
The “**BackUP**” button allows you to save the configuration of the GN-BR404W to a temp file on your PC. You can then click the “**Restore**” button to restore the saved backup configuration file.



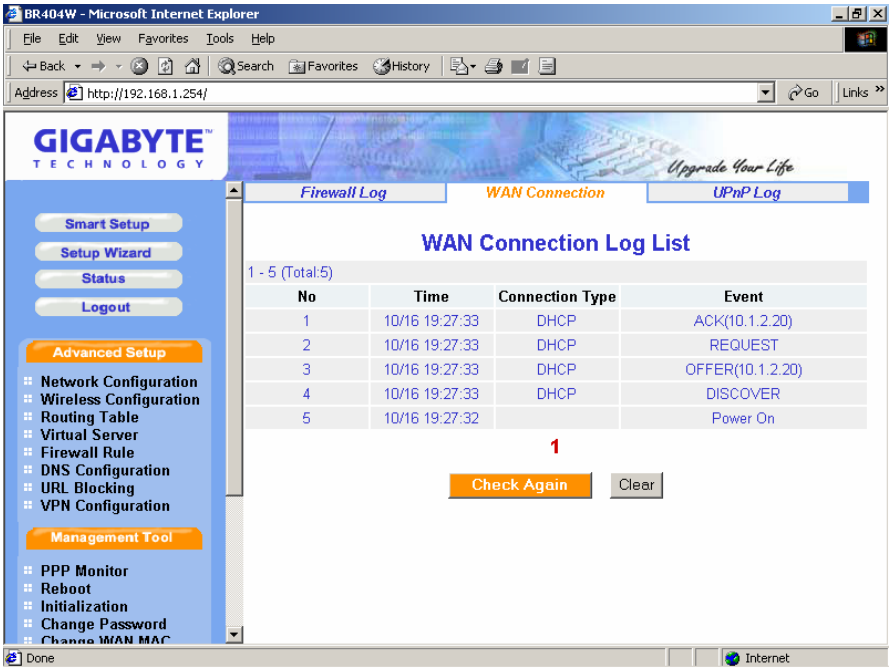
3-5-8. Log Information

From here, you can veiw the record of the firewall log, WAN connection and the UPnP log. If you want to reload the data of the log list, please click "**Check Again**" button.

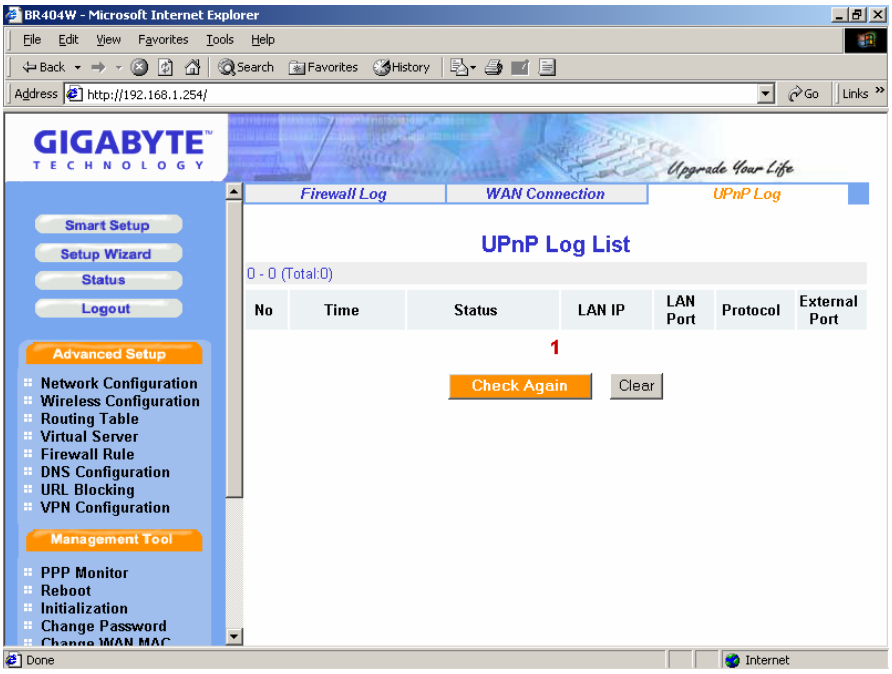
■ Firewall Log



■ WAN Connection

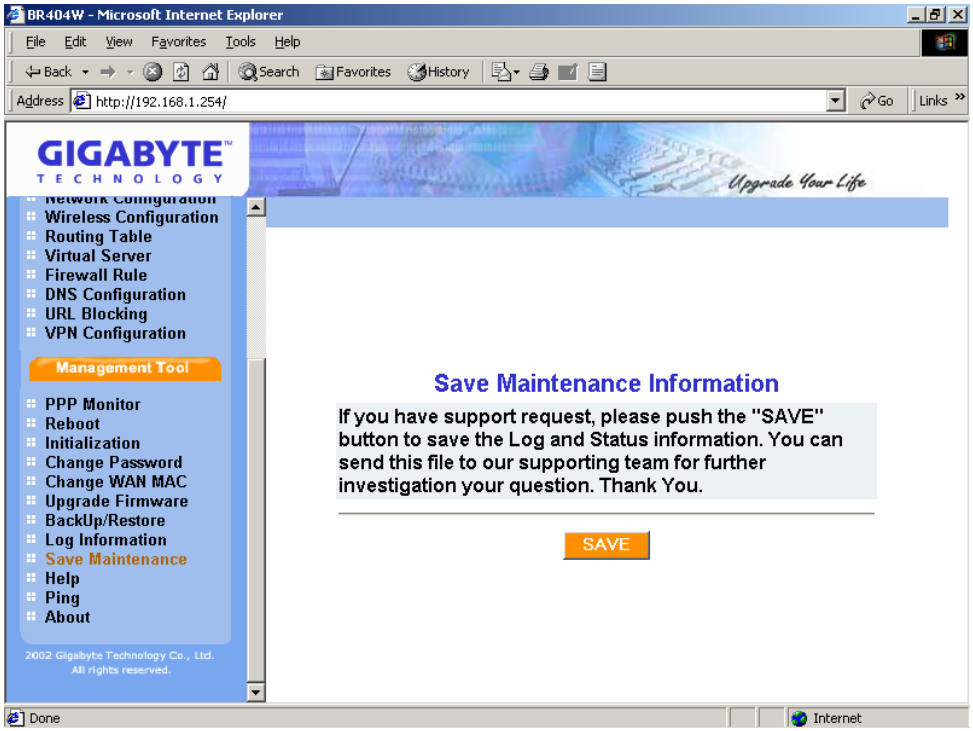


■ UPnP Log



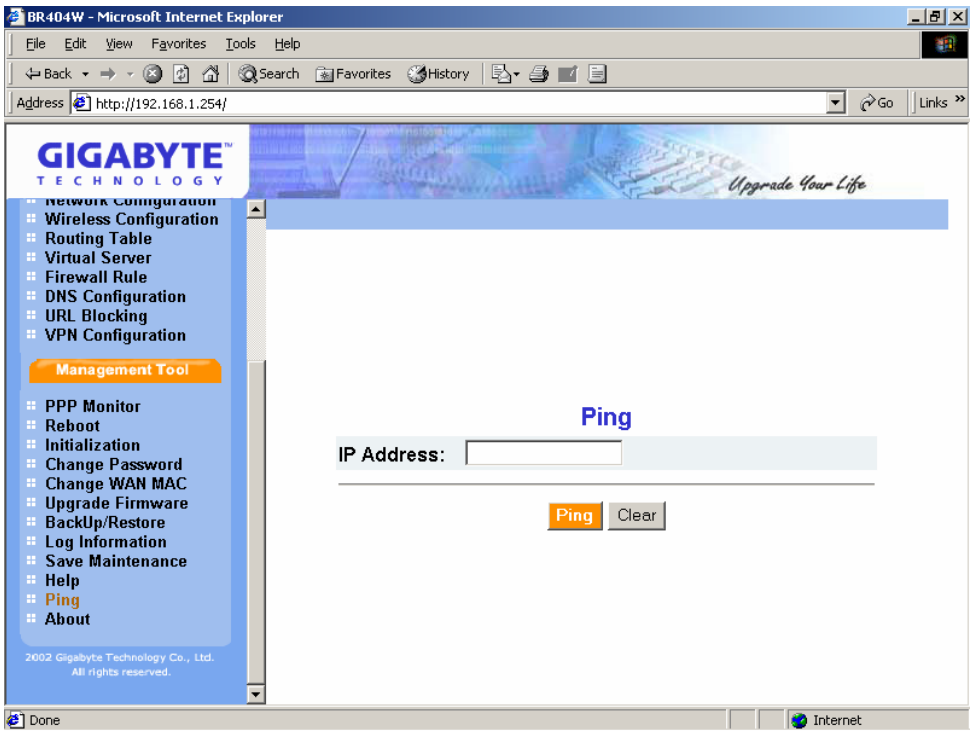
3-5-9. Save Maintenance

Please save the log and the status information if you have the support requirement. And then send this file to Gigabyte supporting team for further investigation your question.



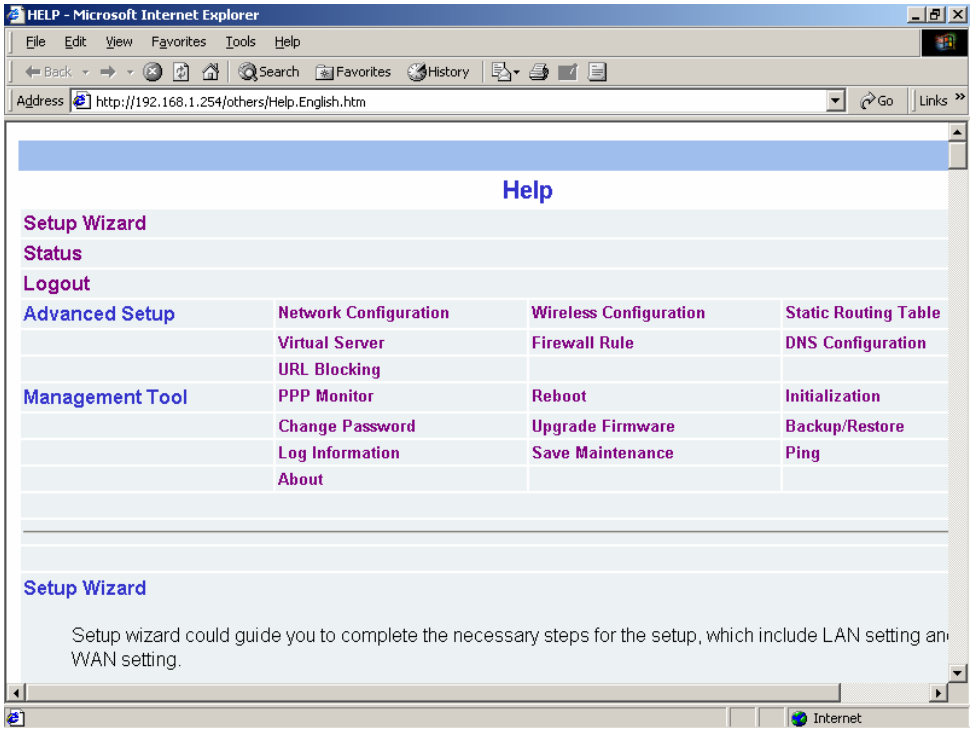
3-5-10. Ping

This “Ping” tool allows you to verify the status of the IP address on the network. Please enter a IP address then click “**Ping**”.



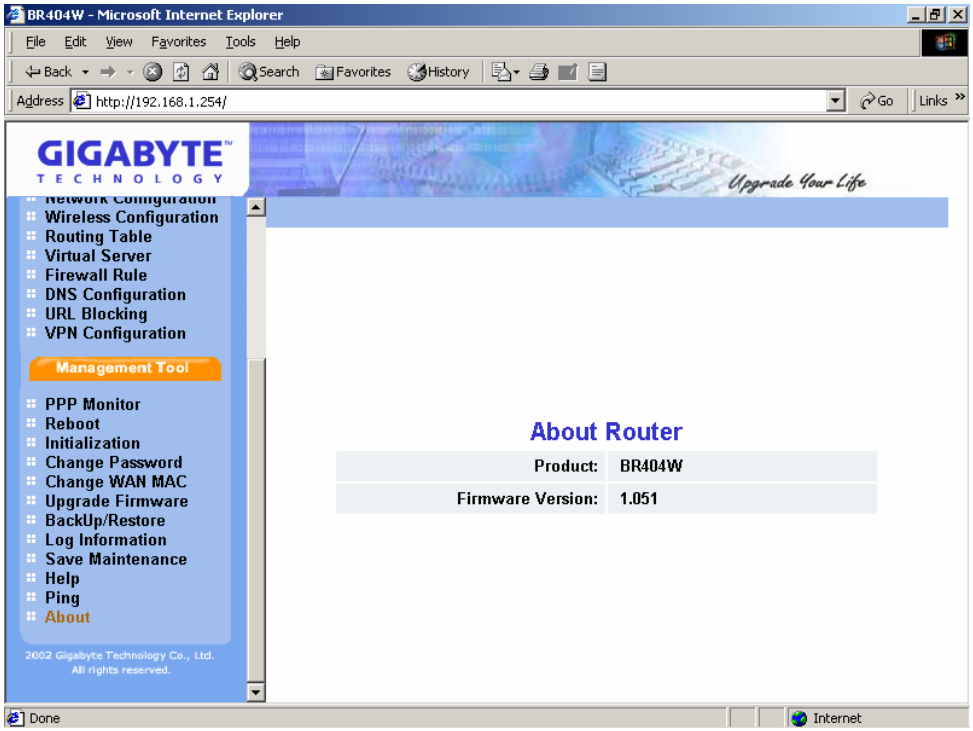
3-5-11 Help

The Help tool can guide you the configuration information of the router.



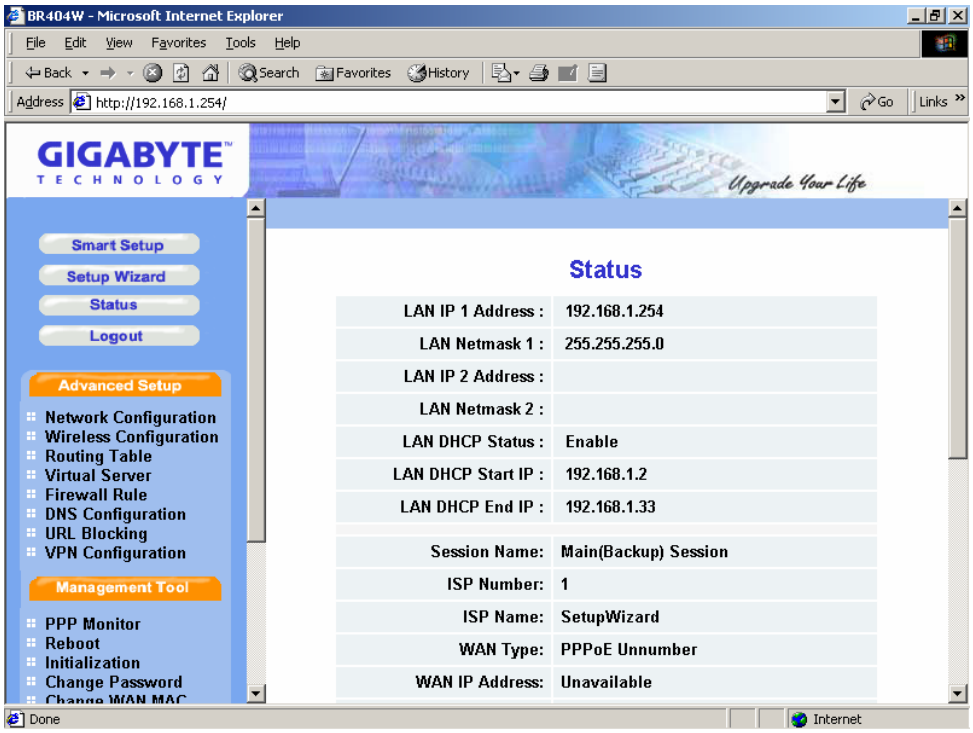
3-5-12 About

This page show you the product name and firmware version.

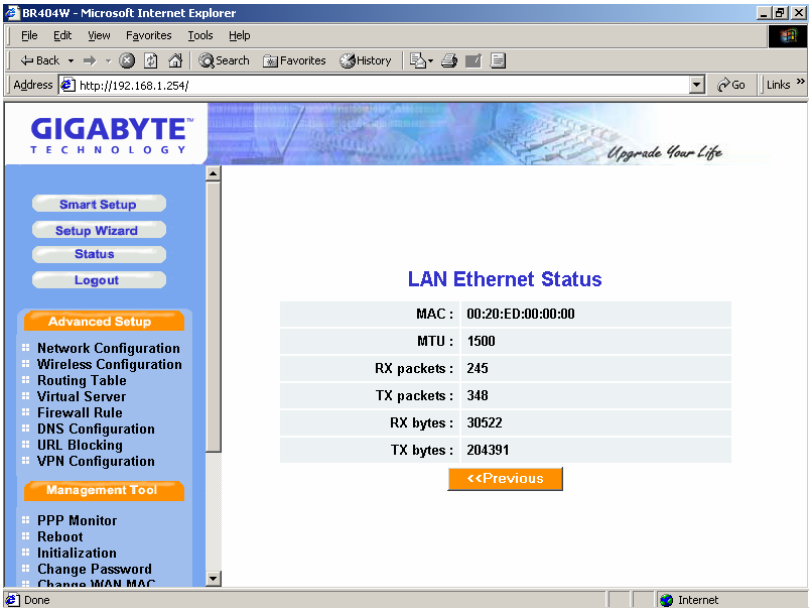


3-6. Status

You can use this status screen to view the router's current connection status.and configuration. The main menu includes LAN information, DHCP information, WAN configuration information, LAN Ethernet Status, WAN Ethernet Status, Wireless Status, ARP Table, DHCP Lease Table, Routing Table and UPnP Mapping Table.



■ LAN Ethernet Status



MAC This field displays the MAC address being used by the LAN port of the router.

MTU The maximum size of the packets sent from your computer onto the network.

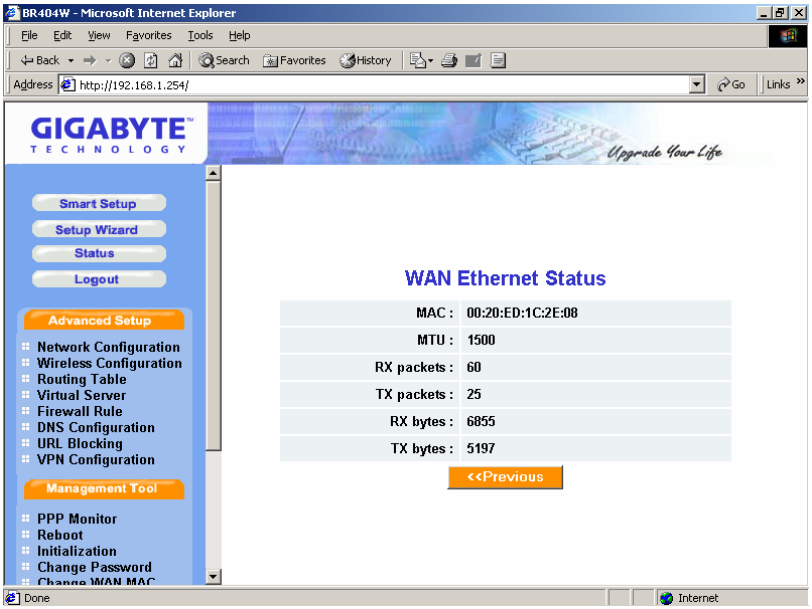
Rx packets The number of the packets received on this port since reset or manual clear.

Tx packets The number of packets transmitted on this port since reset or manual clear.

Rx bytes The current reception bandwidth used on the LAN ports.

Tx bytes The current transmission bandwidth used on the LAN ports.

■ WAN Ethernet Status



MAC This field displays the MAC address being used by the WAN port of the router.

MTU The maximum size of the packets sent from your computer onto the network.

Rx packets The number of the packets received on this port since reset or manual clear.

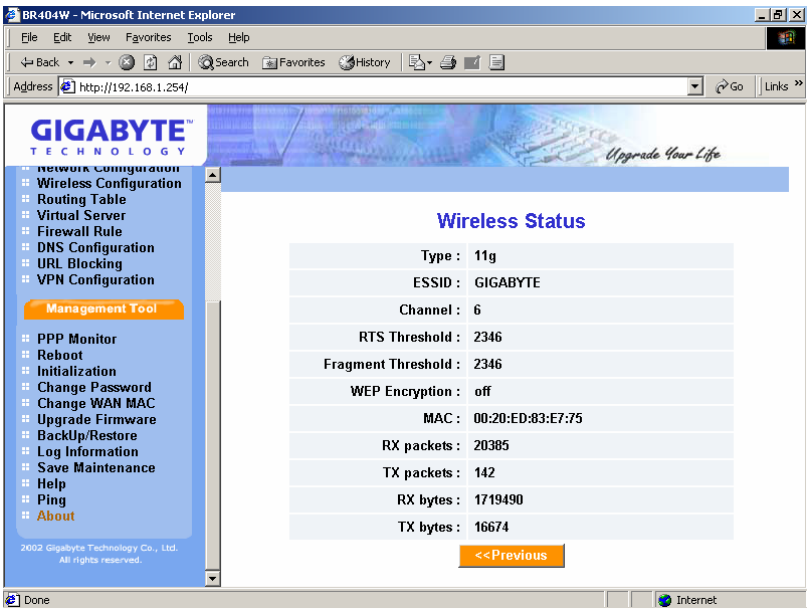
Tx packets The number of packets transmitted on this port since reset or manual clear.

Rx bytes The current reception bandwidth used on the WAN ports.

Tx bytes The current transmission bandwidth used on the WAN ports.

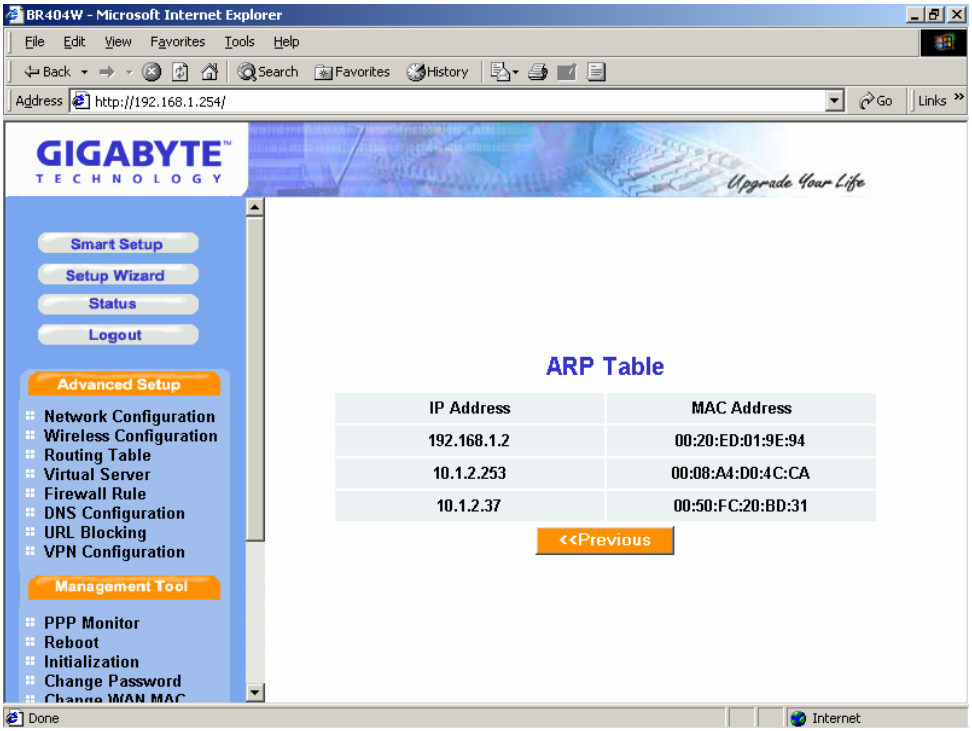
■ Wireless Status

From this page, you can get the current Wireless LAN connection information.



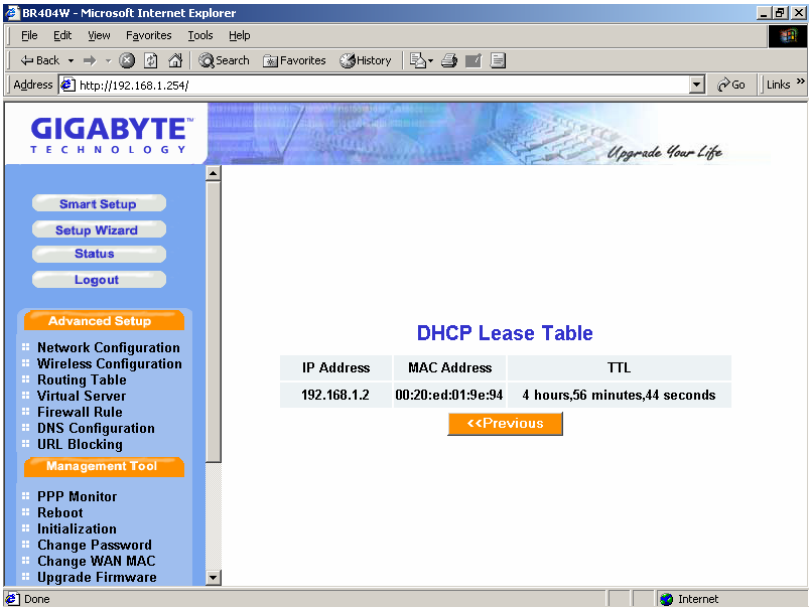
■ ARP Table

The ARP Table will show you the mapping of the IP address and MAC address of the PCs.



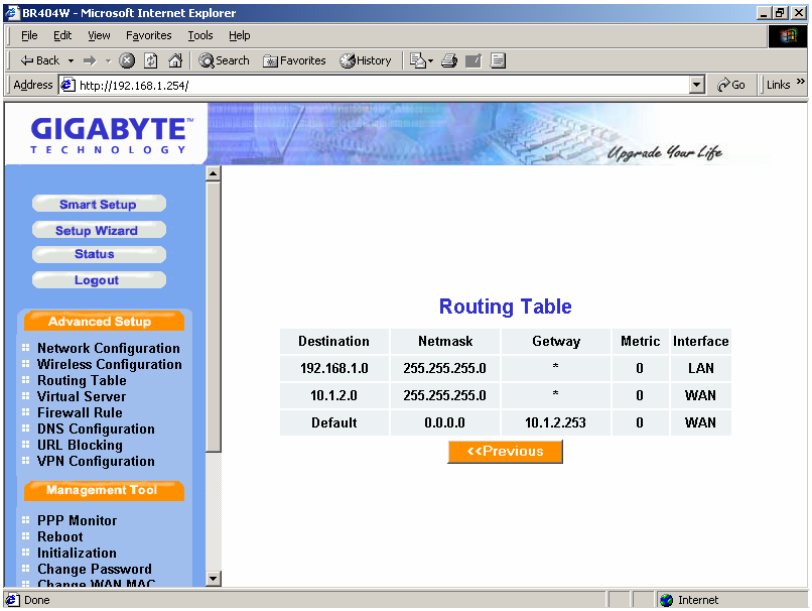
■ DHCP Lease Table

From this table, you can get the information of the IP assignment.



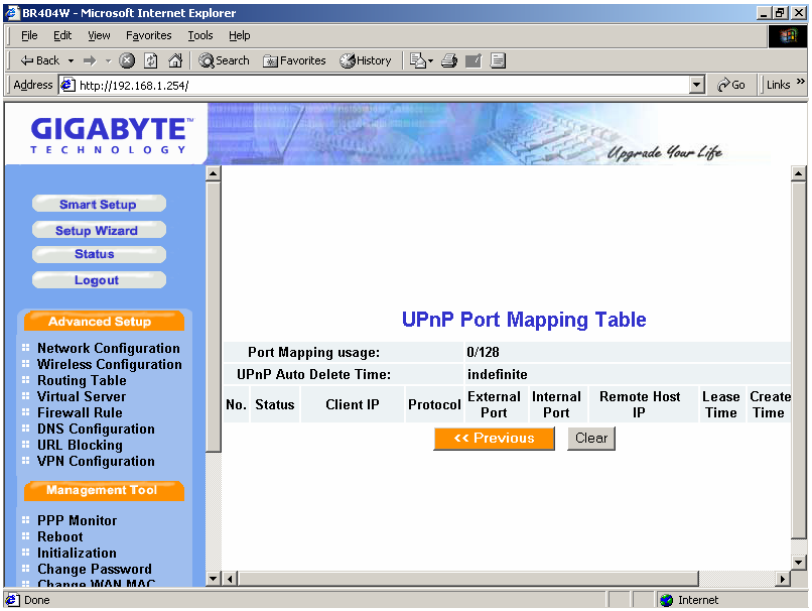
■ Routing Table

The Routing table can show you the routing information of the router.



■ UPnP Port Mapping Table

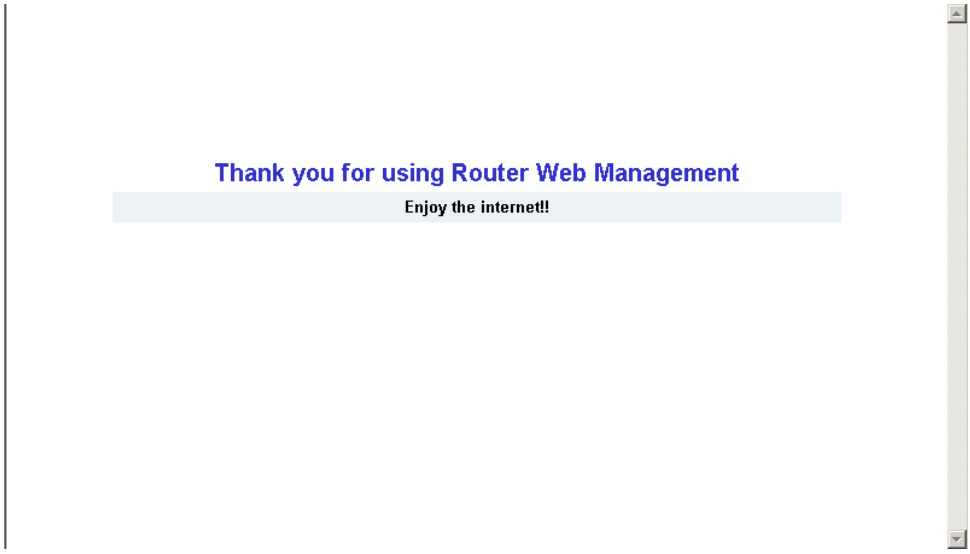
From this table, you can get the UPnP Port Mapping information of the router.



3-7. Logout

As you finished the configuration of the GN-BR404W, please choose “Logout”.

After 5 minutes idle time, the system will be logout automatically.



4. Troubleshooting

This chapter gives information about troubleshooting your wireless broadband router. Read the descriptions below to help you diagnose and solve the problem.

Q: What to do if you forget your password or forget the IP address of the router?

A: Please press the “init” bottom on the router. The router will be restart and the system setting will restore to the default value.

Q: Unable to connect to the Internet?

A: 1. Please confirm whether or not the power cord is connected properly, and the power indicating light of the router is normal.
2. Please confirm whether or not all of the settings described in this manual are set.
3. Please confirm if ADSL or Cable Modem operates properly, and if the ISP network service expires.
4. Please confirm if your network cable is connected properly, and the LED status is normal.

Q: What is the IEEE802.11b standard?

A: It also referred to as 802.11 High Rate or Wi-Fi. It is an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

Q: Unable to access the router’s Web Configuration Interface?

A: 1. Please check the Ethernet connection between the PC and the router is correctness.
2. Make sure your computer’s IP address is on the same subnet as the router.
3. Make sure you are using the correct login information.

Q: Where is the router installed on the network?

A: In a typical environment, the router is installed between the ADSL or Cable Modem and the LAN. Plug the router into the Ethernet port of the ADSL or Cable Modem.

Q: Can the router act as DHCP server?

A: Yes. The router has the DHCP server function built-in.

Q: What is WEP?

A: Wired Equivalent Privacy. Security mechanism defined within the 802.11 standard designed to make the link integrity of the wireless medium equal to wired cable. Data privacy mechanism based on a 40 bits (128 bit optional) shared key algorithm, as described in the IEEE 802.11 standard.

Q: What is the IEEE802.11g standard?

A: IEEE 802.11g standard specifies data rates of up to 54 Mbits/s in the 2.45-GHz band. It uses orthogonal frequency division multiplexing (OFDM), mandatory provisions have been made within the standard to make it inherently compatible with the well-established 802.11b standard at 11 Mbits/s, which uses complementary code keying (CCK) modulation. Both .11g and .11b operate at ranges of up to 300 feet.

Appendix A: Glossary

ADSL
Asymmetric digital subscriber line (ADSL) is a new modem technology that converts existing twisted-pair telephone lines into access paths for high-speed communications of various sorts.

Auto-MDI/MDIX
On a network hub or switch, an auto-MDI/MDIX port automatically senses if it needs to act as a MDI or MDIX port. The auto-MDI/MDIX capability eliminates the need for crossover cables.

Auto-negotiate
To automatically determine the correct settings. The term is often used with communications and networking.

DHCP
The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

DMZ
In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DNS
The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses, and to control Internet email delivery. Most Internet services rely on DNS to work, and if DNS fails, web sites cannot be located and email delivery stalls.

Dynamic IP Address

An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Gateway

A device, usually a router, that connects hosts on a local network to other networks.

IP Address

Every machine on the Internet has a unique identifying number, called an IP Address. A typical IP address looks like this: 216.27.61.137

IPSec

IPSec stands for IP Security. It provides authentication and encryption over the Internet. It functions at Layer 3 and thus secures everything on the network. It has become a standard protocol used for virtual private networks (VPNs).

MAC Address

On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. Usually written in the form 01:23:45:67:89:ab

MTU

The size in bytes of the largest packet that can be sent or received.

NAT

A technique by which several hosts share a single IP addree for access to the Internet.

Ping (Packet Internet Groper)

A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections.

SSID

The SSID is the name represent the router in the wireless network.

PPPoE

Point-to-Point over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Router

A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP network. Routers are located at gateways, the places where two or more networks connect.

Subnet Mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address. Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol), the suite of communications protocols used to connect hosts on the Internet.

VPN

Virtual private networks are secured private network connections, built on top of publicly-accessible infrastructure, such as the Internet or the public telephone network. VPNs typically employ some combination of encryption, digital certificates, strong user authentication and access control to provide security to the traffic they carry. They usually provide connectivity to many machines behind a gateway or firewall.

WAN

Wide Area Network, a communication network that covers a relatively large geographic area, consisting of two or more LANs. Broadband communication over the WAN is often through public networks such as the ADSL or Cable systems, or through leased lines or satellites. In its most basic definition, the Internet could be considered a WAN.

WEP

WEP (Wired Equivalent Privacy) is a data privacy mechanism based on a 64/128-bit shared key algorithm, as described in the IEEE 802.11 standard.

Appendix B: General Public License

Licensing Information

This product includes copyrighted software license owned by third-party under terms of the GNU General Public License. Texts of the GPL are included with every CD shopped with our product. All future firmware updates will also be accompanied with their related source code on our website.

Please refer to the following GNU General Public License for further details of this License.

Specially, the parts of this product listed below are subject to the GNU General Public License.

1. The Linux operating system kernel
2. The iptables packet filter and NAT software
3. The busybox swiss army knife of embedded linux
4. The udhcpd DHCP client/server implementation
5. The rp-pppoe PPPoE client implementation
6. The pppd PPP daemon implementation
7. The ez-ipupdate ddns implementation
8. The zebra routing daemon implementation
9. The iproute2 implementation
10. The PCMCIA card manage implementation
11. The freeswan VPN implementation

The Copyright for All listed Software packages are owned by their respective authors, please refer to the source code via our website for further details.

Availability of Source Code

Gigabyte Tech. has provided the full Source Code of the GPL Licensed Software on our website. All future firmware updates will also be accompanied with their related source code.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.
When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.
To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.
For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.
We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.
Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.
Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.
The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)
These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.
In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.
3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)
The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.
If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.
4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.
If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.
This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY
11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs
If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which

everyone can redistribute and change under these terms.
To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.
one line to give the program's name and an idea of what it does.
Copyright (C) *yyyy name of author*

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
Also add information on how to contact you by electronic and paper mail.
If the program is interactive, make it output a short notice like this when it starts in an interactive mode:
Gnomovision version 69, Copyright (C) *year name of author*
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'. This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.
The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.
You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.
signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Limited Warranty

1-Year Warranty

Gigabyte warrants to the original consumer/purchaser that the product free from defects in material and workmanship for no limited time from the original manufactory shipment date. This warranty does not cover the product if it is damaged in the process of being installed or improperly used.

Gigabyte may replace or repair the product with either new or reconditioned parts. Repaired or replaced products will be returned to you at the same revision level as received or higher at Gigabyte's option. Gigabyte reverses the right to replace discounted products with an equivalent generation product.

KEEP THIS STUB FOR YOUR PURCHASING RECORD

Customer:	
Phone No:	
Address:	
Email:	
Model:	
Serial:	
Date of Purchase:	
Place of Purchase:	
From Whom:	
Distributor:	

Customer Satisfaction

GIGA-BYTE TECHNOLOGY CO., LTD.

No.6, Bau Chiang Road, Hsin-Tien, Taipei Hsien, Taiwan, R.O.C.

Tel: 886-2-89124888

Fax:886-2-89124007

http://www.gigabyte.com.tw

Technical Support

E-mail: networksupport@gigabyte.com.tw